Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Vendor Due Diligence Policy

PURPOSE:
The purpose of this policy is to establish requirements for evaluating, selecting, approving, and monitoring third-party vendors, contractors, consultants, cloud service providers, software providers, and managed service providers that access, store, process, transmit, or support Clarendon College information resources.

This policy helps ensure compliance with:

- Texas Administrative Code Chapter 202 (TAC §202)
- Texas Department of Information Resources (DIR) Security Controls Standards Catalog
- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA), where applicable
- Payment Card Industry Data Security Standard (PCI DSS), where applicable
- Clarendon College Information Security Program

SCOPE:
This policy applies to:

- Technology vendors
- Cloud/SaaS providers
- Software suppliers
- Managed service providers
- Consultants
- Independent contractors
- Third parties processing institutional data
- Vendors receiving network access
- Vendors with remote support access

POLICY STATEMENT:
No vendor shall:

- Access Clarendon College information systems,
- Receive confidential data,
- Connect to institutional networks, or
- Be awarded a technology-related contract

Until *the vendor has completed the due diligence review process and received approval from:*

- Vice President of Information Technology, and
- Vice President of Administrative Services, as appropriate.

Vendor Risk Classification
All vendors will be classified and reviewed according to the risk categories below. These classifications will be noted on the Vendor Risk Assessment Form, see Appendix A. This form will be used to determine the project's acceptable risk.

Low Risk
Examples:

- Public information services
- Office supplies
- Non-networked equipment

Review Requirements:

- Procurement review only

Moderate Risk
Examples:

- Software vendors
- Hosted applications
- Learning applications

Review Requirements:

- Security questionnaire
- Contract review
- Data classification review

High Risk
Examples:

- Student information systems
- Financial systems
- Cloud hosting providers
- Managed service providers
- Vendors accessing confidential data

Review Requirements:

- Comprehensive security review
- Risk assessment
- Contractual security provisions
- VPIT approval

Significant vendor security incidents or critical assessment findings may be reported to executive leadership and the Board of Regents through established governance channels.

Critical Risk
Critical Vendors are vendors whose loss, compromise, or unavailability would significantly impact the College's ability to deliver instruction, maintain operations, process payroll, administer financial aid, manage student records, or meet regulatory requirements.

Examples:

- SIS
- ERP
- LMS
- Identity Provider
- Financial Aid Systems
- Managed Security Providers

Vendor assessments shall evaluate confidentiality, integrity, availability, operational impact, financial impact, and regulatory impact.

Required Due Diligence Documentation
As applicable, vendors shall provide:

Corporate Information

- Company name and ownership
- Primary contacts
- Years in operation
- Financial stability information

Security Documentation
At least one of the following:

- SOC 2 Type II Report
- SOC 1 Report
- ISO 27001 Certification

Where applicable, vendors shall provide evidence of the following, or equivalent security assessment documentation acceptable to Clarendon College:

- TX-RAMP Authorization
- StateRAMP Authorization
- FedRAMP Authorization (if applicable)

Vendors hosting Confidential, Sensitive, FERPA, HIPAA, or financial information should provide evidence of compliance through:

- TX-RAMP certification when required,
- FedRAMP authorization,
- StateRAMP authorization, or
- Comparable third-party assessments approved by Clarendon College IT.

Cyber Insurance Documentation
Minimum requirements:

- $1M Cyber Liability
- Breach Response Coverage

Clarendon College Information Technology Services shall review third-party security documentation and identify any material exceptions, qualified opinions, or unresolved findings.

Security Questionnaire

Vendor must complete a security assessment covering:

- Access control
- Identity management
- Encryption
- Logging and monitoring
- Incident response
- Vulnerability management
- Backup and disaster recovery
- Employee background checks
- Security awareness training

The vendor will be provided with a Vendor Security Questionnaire to be completed before the installation of their service, application, or system. Please see Appendix B, Vendor Security Questionnaire.

Data Protection Information

Vendor must identify:

- Types of college data collected
- Storage locations
- Subprocessors
- Data retention periods
- Data destruction methods

Significant security deficiencies identified during assessment shall require documented remediation or formal risk acceptance.

Contract Security Requirements

Contracts involving institutional data shall include the following items:

Confidentiality

The vendor must protect all Clarendon College confidential information.

Notification Requirements

Vendor shall report:

- Security incidents
- Data breaches
- Unauthorized disclosures

Within:

24 hours of discovery

Right to Audit

Clarendon College reserves the right to:

- Review security documentation
- Request audit reports
- Conduct security assessments when warranted

Data Ownership

All institutional data remains the property of Clarendon College.

Termination Rights

Contracts must be provided for:

- Secure data return
- Data destruction certification
- Removal of vendor access
    - At contract termination.
- FERPA-protected information shall be securely destroyed upon contract termination unless retention is required by law.

Vendor security assessments shall be updated before contract renewal or significant changes to service offerings.

A Data Processing Agreement must be completed before signing any contract. Please see Appendix C, Data Processing Agreement Template, for the agreement requirements.

Cloud Service Requirements

Cloud providers must:

Provide Encryption

- Data in transit
- Data at rest

Demonstrate Security Controls

Consistent with:

- TAC §202
- DIR Security Controls Standards
- NIST SP 800-53

Support Multi-Factor Authentication

- For administrative and privileged access.

Maintain Business Continuity Capabilities

Including:

- Backups
- Disaster recovery
- Incident response procedures
    - Please see Appendix D, Third Party Breach Notification Standard.

All AI projects or projects containing AI will be reviewed in accordance with Appendix F, Artificial Intelligence Vendor Review Addendum.

FERPA, financial aid, employee, and confidential institutional information shall not be used for training Artificial Intelligence foundation models unless explicitly approved by the Vice President of Information Technology and disclosed in a contract.
AI-generated recommendations affecting students shall not be relied upon without human review and validation.

Vendor Access Management
Vendor access shall:

- Be approved by the data owner
- Be limited to least privilege
- Be time-bound where feasible
- Be reviewed annually
- Utilize unique accounts
- Require multi-factor authentication when supported

Shared vendor accounts are prohibited.

Vendors receiving access to student education records shall be considered School Officials under FERPA only when performing institutional services for which Clarendon College would otherwise use employees and when subject to direct institutional control regarding the use and maintenance of education records.

Vendors shall not disclose education records to any unauthorized party and shall be prohibited from redisclosing FERPA-protected information without written authorization from Clarendon College.

Vendors shall only access the minimum education record information necessary to perform contracted services.

Ongoing Monitoring
High-risk vendors shall be reviewed annually.

Reviews may include:

- Updated security questionnaires
- Updated SOC reports
- Breach history reviews
- Contract compliance reviews
- Risk reassessments

Significant findings may result in remediation requirements or contract termination.

The annual review will utilize the checklist from Appendix E, Annual Vendor Review Checklist.

Products used by students, faculty, staff, or the public shall be evaluated for accessibility compliance, including WCAG 2.1 AA and applicable ADA requirements.

Exceptions

Exceptions must:

- Be documented
- Include risk acceptance justification
- Be approved by:
    - Vice President of Information Technology
    - Appropriate Executive Sponsor

Roles and Responsibilities

Vice President of Information Technology

Responsible for:

- Vendor risk assessments
- Security reviews
- Approval recommendations
- Ongoing monitoring

Procurement / Administrative Services

Responsible for:

- Contract management
- Purchasing compliance
- Vendor documentation retention

Data Owners

Responsible for:

- Defining data requirements
- Approving vendor access
- Reviewing business needs

Vendors

Responsible for:

- Providing accurate information
- Maintaining security controls
- Reporting security incidents
- Providing notification for any of the following changes:
    - Ownership changes
    - Hosting changes
    - Data residency changes
    - Security program changes

RELATED POLICIES, REFERENCES, AND ATTACHMENTS:
An index of approved Clarendon College-IT policies is available on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology.html
The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website. Also, please see the following related policies below;

a. Clarendon College's Technology Acquisition Oversight Policy
b. Clarendon College's System Development & Acquisition Policy

The Clarendon College Board of Regents approved this policy on October 22, 2026, version 1.0. This policy was reviewed by Will Thompson, Vice President of IT, on September 29, 2026.

Appendix A

Clarendon College Vendor Risk Assessment Form

Vendor Name: _____
Product/Service Name: _____
Business Owner/Department: _____
Vendor Contact: _____
Date Submitted: _____
Contract Value: _____
Contract Term: _____
Assessment Conducted By: _____

Vendor reviews shall incorporate the requirements of Clarendon College's Data Classification Policy and Information Security Program.

Section 1: Service Description
Purpose of Service
Describe the service and intended business use.

Hosting Model
☐ SaaS (Cloud Hosted)
☐ On-Premises
☐ Vendor Hosted
☐ Hybrid
☐ Other: _____

Vendor Access
Will vendor personnel have access to Clarendon College systems?
☐ Yes
☐ No
If yes, describe:

Section 2: Data Classification
What types of college data will the vendor access, store, process, transmit, or support?

Data Type	Yes	No
Public Information	☐	☐
Internal Business Information	☐	☐
FERPA Student Records	☐	☐
Financial Data	☐	☐
HR/Employee Data	☐	☐
HIPAA/Health Data	☐	☐
Payment Card Data	☐	☐
Research Data	☐	☐
Other Confidential Data	☐	☐

If confidential data will be used, describe:

Section 3: Security Controls Review

Authentication

Question	Yes	No
Supports Multi-Factor Authentication (MFA)	☐	☐
Supports Single Sign-On (SSO)	☐	☐
Unique user accounts required	☐	☐
Role-based access controls are available.	☐	☐

Encryption

Question	Yes	No
Data encrypted in transit.	☐	☐
Data encrypted at rest.	☐	☐
Encryption keys are managed securely.	☐	☐

Security Operations

Question	Yes	No
Security monitoring performed	☐	☐
Vulnerability scanning performed	☐	☐
Annual penetration testing conducted	☐	☐
A security incident response program exists.	☐	☐
Log retention available	☐	☐

Business Continuity

Question	Yes	No
A formal backup process exists.	☐	☐
A disaster recovery program exists.	☐	☐
Recovery testing is performed annually.	☐	☐

Section 4: Compliance Documentation

Indicate which documents have been obtained.

Document	Received
SOC 2 Type II Report	☐
SOC 1 Report	☐
ISO 27001 Certificate	☐
StateRAMP Authorization	☐
FedRAMP Authorization	☐
Cyber Liability Insurance Certificate	☐
Security Questionnaire	☐
Data Processing Agreement	☐
Business Associate Agreement (HIPAA)	☐
FERPA Compliance Statement	☐

Accessibility Review (WCAG/ADA)	☐

Section 5: Data Management
Data Storage Location
Country/Region:

Subprocessors Used
☐ Yes
☐ No

If yes, list:

Data Retention
How long is data retained?

Data Destruction
Describe the destruction process:

Section 6: Incident Response
Security Event Notification
Can the vendor notify Clarendon College within 24 hours of discovery?
☐ Yes
☐ No

Has the Vendor Experienced a Breach in the Last 5 Years?
☐ Yes
☐ No

If yes, explain:

Section 7: Artificial Intelligence Review
(Required for systems using AI, machine learning, or generative AI.)

Question	Yes	No
Product uses AI or machine learning.	☐	☐
College data used to train models.	☐	☐
Customer data is isolated from other customers.	☐	☐
Data can be excluded from model training.	☐	☐
Humans can review AI decisions.	☐	☐

Additional comments:

Section 8: Risk Scoring

Confidential Data

- No Confidential Data = 0 points
- FERPA Data = 10 points
- Financial Data = 10 points
- HIPAA Data = 15 points
- Payment Card Data = 15 points

Security Controls

- No MFA = 10 points
- No Encryption at Rest = 15 points
- No Penetration Testing = 10 points
- No Incident Response Plan = 15 points

Vendor Access

- Remote Administrative Access = 15 points
- Network Access = 10 points

Compliance Documentation

- No SOC/ISO/Equivalent Assessment = 10 points

Total Score: _____

Risk Ratings

Score	Classification
0-20	Low Risk
21-50	Moderate Risk
51-80	High Risk
81+	Critical Risk

Section 9: Review Determination

Recommended Risk Level

☐ Low
☐ Moderate
☐ High
☐ Critical

Recommendation

☐ Approved
☐ Approved with Conditions
☐ Pending Remediation
☐ Denied

Required Corrective Actions

Review Notes

Section 10: Approvals
Business Owner
Name: _____

Signature: _____
Date: _____

Information Technology Review
Name: _____

Signature: _____
Date: _____

Vice President of Information Technology
Name: _____

Signature: _____
Date: _____

Section 11: Automatic review matrix:
Low Risk → Department Approval + IT Review
Moderate Risk → IT Security Review Required
High Risk → VP of IT Approval Required
Critical Risk → VP of IT + President/Administrative Services Approval Required

Appendix B

Vendor Security Questionnaire

General Information
Vendor Name: _____
Product/Service: _____
Primary Contact: _____
Date Completed: _____

Organization Security
1. Do you maintain a formal information security program?
☐ Yes
☐ No

2. Do you have a designated Information Security Officer?
☐ Yes
☐ No

3. Are security policies reviewed annually?
☐ Yes
☐ No

4. Do employees receive annual security awareness training?
☐ Yes
☐ No

5. Are background checks performed on employees with access to customer data?
☐ Yes
☐ No

6. Do you maintain a Secure Software Development Lifecycle (SSDLC)?
☐ Yes
☐ No

7. Are developers trained in secure coding practices?
☐ Yes
☐ No

8. Is the source code reviewed before production deployment?
☐ Yes
☐ No

9. Do you perform software composition analysis (SCA)?
☐ Yes
☐ No

10. Do you maintain a software bill of materials (SBOM)?
☐ Yes
☐ No

Access Control
1. Is Multi-Factor Authentication required for administrative accounts?
☐ Yes
☐ No

2. Does the system support SSO (SAML, Azure AD, Entra ID)?
☐ Yes
☐ No

3. Are privileged accounts reviewed periodically?
☐ Yes
☐ No

4. Are shared accounts prohibited?
☐ Yes
☐ No

Data Protection
1. Is data encrypted at rest?
☐ Yes
☐ No

2. Is data encrypted in transit?
☐ Yes
☐ No

3. What encryption standards are used?_____

4. Describe data retention practices:

5. Describe data destruction procedures:

Vulnerability Management
1. Are vulnerability scans performed?
☐ Yes
☐ No

2. Frequency:

☐ Weekly

☐ Monthly

☐ Quarterly

3. Are annual penetration tests conducted?

☐ Yes

☐ No

4. Are critical vulnerabilities remediated within 30 days?

☐ Yes

☐ No

Incident Response

1. Do you maintain a written incident response plan?

☐ Yes

☐ No

2. When were incident response procedures last tested?_____

3. Can Clarendon College be notified within 24 hours of discovery of a security incident?

☐ Yes

☐ No

Compliance

Check all that apply:

☐ SOC 2 Type II

☐ SOC 1

☐ ISO 27001

☐ TX-RAMP

☐ StateRAMP

☐ FedRAMP

☐ FERPA Acknowledgment

☐ HIPAA Compliance

☐ PCI-DSS

Appendix C

Data Processing Agreement (DPA) Template

Purpose
This Data Processing Agreement ("DPA") governs the processing of institutional information by the Vendor on behalf of Clarendon College.

Definitions
College Data means any information provided to Vendor by Clarendon College, including:

- Student records
- Employee records
- Financial information
- Research information
- Confidential institutional information

Data Ownership

- All College Data remains the sole property of Clarendon College.
- Vendor shall acquire no ownership rights in Clarendon College Data.

Authorized Processing

- Vendor shall process Clarendon College Data only:
- For contracted services
- In accordance with documented Clarendon College instructions or policies
- In accordance with applicable laws

Confidentiality
Vendor shall ensure all personnel:

- Maintain confidentiality
- Complete security awareness training
- Are bound by confidentiality obligations

Security Controls
Vendor shall maintain:

- MFA for privileged access
- Encryption in transit
- Encryption at rest
- Vulnerability management processes
- Incident response capabilities
- Audit logging

Subprocessors
Vendor shall:

- Disclose all subprocessors
- Obtain written approval before adding new subprocessors
- Flow down equivalent security requirements

Security Incidents
Vendor shall notify Clarendon College within:
24 hours of becoming aware of a Security Incident.

Please refer to Appendix D, Third-Party Breach Notification Standard.

Notification shall include:

- Date discovered
- Systems impacted
- Types of affected records
- Corrective actions
- Planned remediation

Audit Rights
Clarendon College may request:

- Security assessments
- SOC reports
- Compliance attestations
- Penetration test summaries

Data Return and Destruction
Upon termination:

Vendor shall:

- Return all Clarendon College Data.
- Securely destroy remaining copies.
- Provide written destruction certification.

Appendix D

Third-Party Breach Notification Standard

Purpose
To establish requirements for reporting cybersecurity incidents involving third parties.

Reporting Timeline

Severity	Notification Requirement
Critical	Within 24 Hours
High	Within 24 Hours
Moderate	Within 72 Hours
Low	At Next Scheduled Review

Reportable Events
Vendor must notify Clarendon College of:

- Unauthorized access
- Data disclosure
- Ransomware incidents
- Malware infections
- Credential compromises
- Denial-of-service attacks
- Vendor subcontractor breaches

Loss of encrypted or unencrypted institutional data

Required Notification Information

- The vendor shall provide:
- Date of incident
- Date discovered
- Systems affected
- Data involved
- Number of affected records
- Containment actions
- Recovery progress
- Law enforcement involvement
- Planned remediation

College Escalation Procedures
Vendor reports shall be sent to:

- Vice President of Information Technology
- Information Security Officer (if designated)
- College Executive Leadership as warranted

Appendix E

Annual Vendor Review Checklist

Vendor Information
Vendor: _____
Assessment Date: _____
Reviewer: _____

Documentation Review

Item	Current	Missing
Contract	☐	☐
DPA	☐	☐
SOC Report	☐	☐
Cyber Insurance	☐	☐
Security Questionnaire	☐	☐

Security Review

Question	Yes	No
Major security incidents this year?	☐	☐
Significant architecture changes?	☐	☐
New subprocessors added?	☐	☐
Compliance reports updated?	☐	☐
Penetration testing completed?	☐	☐

Business Review

Question	Yes	No
Services still required?	☐	☐
Performance acceptable?	☐	☐
Costs remain reasonable?	☐	☐
Alternative products evaluated?	☐	☐

Review Outcome
☐ Continue Service
☐ Continue with Corrective Actions
☐ Increased Monitoring
☐ Contract Termination Recommended

Appendix F

Artificial Intelligence Vendor Review Addendum

Purpose:
Required for any solution containing Artificial Intelligence, Machine Learning, Generative AI, Large Language Models (LLMs), Predictive Analytics, or Automated Decision-Making.

Also see the Clarendon College Cloud Computing Policy:
https://www.clarendoncollege.edu/Resources/IT/2025/CloudComputingPolicy1.pdf.

Section 1: AI Data Usage

1. Does the vendor use data from Clarendon College to train AI models?

☐ Yes
☐ No

2. Can model training be disabled?

☐ Yes
☐ No

3. Is customer data isolated from other customers?

☐ Yes
☐ No

4. Is College data used for product improvement?

☐ Yes
☐ No

5. Explain how institutional data is used:

Section 2: Data Residency

1. Where is the college data stored?

☐ United States
☐ Multiple Countries
☐ Unknown
Location(s):_____

2. Can data residency be restricted to the United States?

☐ Yes
☐ No

3. Are backups stored outside the United States?

☐ Yes
☐ No

Section 3: Model Transparency

5. Can the vendor identify which AI models are used?

☐ Yes

☐ No

6. Does the vendor provide documentation regarding:

Topic	Yes	No
Training Methodology	☐	☐
Model Limitations	☐	☐
Bias Testing	☐	☐
AI Governance Program	☐	☐
Human Review Controls	☐	☐

7. Can users challenge or override AI-generated outputs?

☐ Yes

☐ No

Section 4: FERPA Impact Assessment

1. Will student education records be processed?

☐ Yes

☐ No

2. Will AI generate recommendations or decisions affecting students?

☐ Yes

☐ No

3. Will AI be used for:

Function	Yes	No
Admissions	☐	☐
Advising	☐	☐
Financial Aid	☐	☐
Academic Evaluation	☐	☐
Student Conduct	☐	☐

4. Can AI outputs be reviewed and corrected by college personnel?

☐ Yes

☐ No

5. Does the vendor contractually prohibit use of FERPA-covered data for model training?

☐ Yes

☐ No

6. AI Risk Determination

Condition	Risk Points
Uses College Data for Training	25
Data Stored Outside U.S.	20
No Human Review Available	20
FERPA Data Processed	15
No Model Transparency	15
No Training Opt-Out	15

AI Risk Rating

- 0-20 = Low
- 21-40 = Moderate
- 41-60 = High
- 61+ = Critical

7. Required Approvals based on the AI Risk Determination Score

AI Risk Level	Approval Required
Low	Department + IT
Moderate	IT Security Review
High	Vice President of IT
Critical	Vice President of IT + President + Legal Review