Payment Card Industry Data Security Standards

Berea College is committed to compliance with the Payment Card Industry (PCI) Data Security Standard, a standard adopted internationally by the major credit/debit card (card) brands (e.g., Visa, MasterCard, Discover, and American Express) to protect card data, regardless of where that data is processed or stored ("PCI Standard").

Scope

This policy governs only those Berea College accounts that were authorized and created under this policy. Unauthorized card activity is prohibited and subject to disciplinary action.

Roles and Responsibilities

Office of Financial Affairs (OFA) – is responsible for implementation and oversight of this policy and general compliance with the PCI Standard, and:

- Establishing and closing merchant accounts. A merchant account is a type of bank account that allows businesses to accept payments by cards;
- Establishing and maintaining relationships with the card payment processing providers and issuing banks. The College currently has a sole source contract with Vantiv for card merchant services; all other forms of electronic payment (PayPal, Google Pay, Apple Pay, etc.) must specifically be approved by the OFA;
- Approving any Point of Sale (POS) device or system to be used within the College;
- Defining the methods of transacting online payments on behalf of the College;
- Maintaining an inventory of all Berea College departments that process card transactions using a College approved merchant account;
- Coordinating with Information Systems and Services (IS&S), as necessary, to review network segmentation configurations and other technical safeguards;
- Coordinating with the Internal Auditor to monitor and audit compliance with this policy and PCI training/education;
- Enforcement of this policy and the PCI Standard including immediate suspension or termination of the ability to process or store cards if a department fails to comply with this policy or the PCI Standard; and
- Other duties related to PCI Compliance as determined by the College.

The OFA, at its discretion, may revoke a merchant account immediately for failure to comply with this policy or the PCI Standard. Revocation of a merchant account will preclude the department from being able to process card transactions.

Departments processing cards – all departments that accept cards must protect card data in compliance with this policy and the PCI Standard. All departments that process card data will implement the business standards described in Appendix C.

All employees responsible for handling card information and/or processing card transactions must have a successful background check on file with either the Human Resources department or their supervisor.

Departments that processed cards prior to the effective date of this policy must initiate compliance efforts with this policy and the PCI Standard within 60 days of policy issue date in order to continue to process cards.

Information Systems and Services (IS&S) – is responsible for:

- approving network segmentation configurations performed in compliance with this policy and the PCI Standard in conjunction with the OFA;
- assisting departments with network segmentation configuration;
- assisting OFA in reviewing vendor contracts, including technology requirements;
- coordinating appropriate vulnerability scanning of Berea College systems that transmit, generate or otherwise access card information;
- assisting investigations relating to security incidents; and
- performing other monitoring and reviews of computer and/or computer networks to ensure that security features are in place and are adequate to protect card data;
- assisting the Internal Auditor with the annual PCI Self-Assessment Questionnaire.

Internal Auditor – The Internal Auditor is responsible for conducting audits of internal controls to confirm compliance with this policy and the PCI Standard and to enforce its provision. The Internal Auditor is responsible, in collaboration with IS&S, for coordinating the annual PCI Self-Assessment Questionnaire with card accepting departments. The Internal Auditor also handles, in collaboration with the General Counsel, any notifications or disclosures required under law or regulation as a result of a security incident.

Department Heads/Managers – Department heads or manager of those areas accepting card transactions are to serve as the liaison between that respective department, the OFA, and IS&S on matters related to card technology strategy and security. This individual, along with the respective vice president, is responsible for completing the PCI Pre-Qualification Form, reviewing and approving the PCI Security Safeguards (Appendix A), and assisting the Internal Auditor with the annual PCI Self-Assessment Questionnaire. Departments are also responsible for covering any applicable card processing fees.

Procedures

For comprehensive procedures involving establishing merchant accounts, the PCI Pre-Qualification Form, department changes to how cards are processed, PCI training, use of

authorized POS systems, use of third party websites, and closing merchant accounts, see Appendix B.

Third Party Vendor Risk Management

Before anyone at Berea College executes or renews an agreement with any third party vendor that processes, transmits, generates, stores or otherwise accesses card data on the College's behalf, the department should request a copy of the vendor's most current PCI compliance attestation and SSAE16 SOC report(s) for the specific services being provided to the College; these documents should accompany the draft vendor contract and applicable Software Acquisition Checklist. In addition, the department is required to monitor and report to the Internal Auditor the vendors' PCI Standard compliance status at least annually.

Card Security Breach

A "security breach" is an unauthorized acquisition of card data that compromises the security, confidentiality or integrity of information maintained by Berea College and covered under this policy. This includes breaches that involve physical security as well as computer or information systems security and also could include unauthorized access to Berea College wireless services.

Any College employee aware of an actual or suspected information security breach must report it immediately to his/her respective manager and the Berea College Internal Auditor.

Departments may not conduct their own investigation without first consulting and coordinating with the Internal Auditor and General Counsel. For further details about the incident response process, please see the Berea College Incident Response Plan and related appendix.

Annual Review

This policy will be reviewed on an annual basis in accordance with the PCI Standard. In addition, departments that process card data will submit a Self-Assessment Questionnaire, network diagram, card flow diagram, and signed PCI Security Safeguards (Appendix A) annually. Individuals who handle card data must complete education specific to the PCI standard annually. In addition, the College will conduct a risk assessment in connection with PCI compliance that identifies threats and vulnerabilities.

Enforcement

All College faculty, staff, student workers and other employees must comply with this policy and the PCI Standard or be subject to disciplinary action in accordance with the Employee Handbook (and related student labor policies), up to termination or expulsion.

Resources

www.pcisecuritystandards.org

Enclosed Forms

PCI Pre-Qualification Form

Enclosed Appendices

Appendix A – PCI Security Safeguards

Appendix B – Procedures

Appendix C – Business Standards

BEREA COLLEGE PCI PRE-QUALIFICATION FORM

New Process___ Change Process___ Date:_____

Please complete all of the information requested below. The form will not be reviewed until all information is provided.

A. Contact Information

1. Name of Departmental Contact/Owner:
   Email Address:
   Cell phone number:

2. Name of Responsible IS&S Liaison:
   Email Address:
   Cell Phone Number:

3. Department:

4. Merchant ID(s):

B. Network Connection. Please indicate if the standard Berea College PCI specific network and services will be used. If not, please contact IS&S for assistance with options and costs for a compliant network connection.

C. Payment Card Flow Diagram. Please attach a current card flow process which shows how cardholder data flows across systems and networks, along with any technical documentation or descriptions that the vendor can provide to assist the College in understanding the physical process of receiving, processing and transmitting card data.

D. Business Purpose:

What is the business purpose for requesting permission to process card transactions?

E. How will card information be obtained? Please select all that apply.

1. In-person
2. Phone
3. Mail
4. Facsimile
5. Email
6. Website

BEREA COLLEGE PCI PRE-QUALIFICATION FORM

F. How will card information be processed? Please select all that apply.

1. Dial-up Terminal
2. IP Terminal
3. Wireless Terminal
4. POS-Purchased System
5. POS – Customized System
6. Berea College Hosted Website
7. Third party Hosted Website

G. If a third party is processing card information on your behalf, please provide the name below (i.e., if you are licensing a third party POS system and/or a third party is hosting the website)

Name of third party: _____

Third Party Contact: _____

Title of Third Party Contact: _____

H. If a third party is processing, storing or otherwise accessing cards on Berea College's behalf, has the applicable Software Acquisition Checklist, including vendor PCI attestation and SSAE16 SOC report(s) been attached?

Yes (If Yes, please provide copy)

No (If No, please explain and provide expected date of completion)

Not Applicable

I. Will Card Data Be Stored? Please select all that apply.

1. No
2. Yes, via paper
3. Yes, electronically and unencrypted
4. Yes, electronically and encrypted
5. Don't know
6. If Yes, please describe:
   a) If any sensitive card data will be stored (full account number, CVV code, PIN);
   b) The purpose for storing the card data;
   c) The length of time that the data will be stored;
   d) How is the data being secured;
   e) How and when will the card data be redacted and/or destroyed.

BEREA COLLEGE PCI PRE-QUALIFICATION FORM

J. In what locations will cards be processed? Check all that apply.

1. Online
2. Berea College – give address
3. Other – describe

K. List all individuals who will handle card information and/or process cards (list individuals who have not otherwise been provided in prior submissions):

L. Have all of these individuals completed PCI Training?

1. Yes
2. No (If No, please provide expected date of completion)
3. Don't Know

M. List all of the devices that will be used to process cards:

1. Laptop
2. Mobile device
3. Workstation
4. Other _____

N. Has the PCI Security Safeguards (Appendix A of the Berea College PCI Policy) been signed? Please provide a copy.

I certify that the above information provided is accurate and complete and that I will promptly update this information in the event of any changes.

_____ _____

Departmental Contact/Owner Printed Name and Signature Date

_____ _____

Vice President of Dept. Printed Name and Signature Date

BEREA COLLEGE PCI PRE-QUALIFICATION FORM

Reviewed & Approved by:

Chief Information Officer Printed Name and Signature	Date
Internal Auditor Printed Name and Signature	Date
Controller Printed Name and Signature	Date
Vice President for Finance Printed Name and Signature	Date

Appendix A PCI Security Safeguards

Any department that processes cards agrees that it has implemented and will maintain the following security safeguards:

1. Card data is not stored in any format (e.g., electronic, hard copy) post-authorization absent written approval from the OFA and IS&S. In no event are CVV, PIN and expiration data stored.

2. Hard copy materials containing card data (and approved by the OFA) have appropriate physical safeguards, including the following:

    - Card data is only retained for the minimum time necessary for its particular purpose;
    - Card data is stored in a secured and locked container (e.g., locker, cabinet, desk, storage bin) and access is restricted to those who are authorized to use the card data;
    - Card data is not removed from the premises; and
    - Card data is destroyed using a cross cut shredder when storage is no longer required.

3. All e-commerce transactions are processed through a third party hosted website approved by the OFA and IS&S, via the Software as a Service (Saas) Checklist.

4. POS systems are segmented from other Berea College systems as confirmed by IS&S.

5. Workstations used to enter card transactions are segmented from other Berea College systems as confirmed by IS&S.

6. Stand-alone card terminals process through analog phone lines or wireless cellular connection and are not permitted to process over an internet connection absent written approval by the OFA and IS&S.

7. Any technology used to access card data is authenticated via dual factor authentication as necessary, as determined by IS&S.

8. Cardholder data must be protected during transmission through the use of strong encryption. Cardholder data is not to be sent or received via email, instant messaging, or other end-user messaging technology.

9. All servers, workstations and mobile devices comply with the College's Network Infrastructure Use policy and the PCI standard, specifically regarding password management, access controls, anti-virus protection, patch management, audit log retention and physical security standards.

10. Mobile devices (laptops, iPads, thumb drives, etc.) are not permitted to process, store or transmit cardholder data absent written approval by the OFA and IS&S.

11. All servers and workstations with access to cardholder data are scanned quarterly and findings are fully remediated. Audit logs are monitored on a regular basis and incidents addressed as required by the PCI Standard and Berea College policies.

12. All servers and third party systems that generate or transmit card data meet the Berea College hardening checklist requirements, as applicable.

13. Employees with access to card data are not permitted to directly access their workstations or laptops, where card transactions are processed, remotely without written approval from IS&S and in no event unless they use VPN.

Reviewed and approved by:

Signature of Vice President of Dept.	Signature of Department Head/Manager
Print Name:	Print Name:
Date:	Date:

Appendix B Procedures

1. Establishing merchant accounts**:** A department must obtain a merchant account from the OFA before accepting cards. A merchant account must be renewed annually. Before providing or approving a change to a merchant account, the OFA will require, as described below:
   a) A completed PCI Pre-Qualification form, as described in #2 below;
   b) Network diagram;
   c) Card flow diagram;
   d) Signed PCI Security Safeguards (Appendix A);
   e) Completion of PCI training by all Berea College employees who processes cards;
   f) Documentation supporting Third Party Vendor PCI compliance (see policy section on Third Party Vendor Risk Management); and
   g) Annual renewal requirements (see policy section on Annual Review).

2. PCI Pre-Qualification form: Any Berea College department that wants to accept cards must complete and submit a PCI Pre-Qualification form to the OFA and IS&S. The form requires, among other things:
   a) A list of devices/methods and Berea College personnel by title authorized to use such devices/methods to process or otherwise access card information; and
   b) A legitimate business reason for the request to process card transactions. The form also must be signed by the vice president of the respective department.
   c) Departments may not begin to process cards until the OFA and IS&S have given written approval.

3. Department changes to how cards are processed**:** Departments must submit to the OFA a revised pre-qualification, network connection description, payment card data flow process, and PCI Security Safeguards (Appendix A) form any time they propose to change the devices or methods used to process cards. The OFA must approve the change in writing before the department can implement the change. If a school or department is uncertain whether a particular change triggers this requirement, contact the OFA for guidance.

4. PCI Security Safeguards (Appendix A): Any Berea College department that wants to accept cards must agree to comply with the security criteria set forth in Appendix A. The PCI Security Safeguards must be renewed annually from the date of signature.

5. PCI training: All Berea College employees (including all faculty, staff, student workers and other employees) and affiliated contractors who handle card data must complete the College's PCI training program before they will be permitted to access or process card data. In addition, training must be completed every fiscal year. As part of the annual training, employees handling card data must acknowledge that they have read and understand this policy. The department is responsible for maintaining a list of employees who handle card data and will provide it to the OFA or the Internal Auditor upon request. The OFA/Internal Auditor will provide training, maintain training records, and approve any exceptions in writing.

6. Use of authorized POS system: Any Berea College department that wants to accept cards through a point of sale ("POS") device or system must use a POS system authorized and approved in writing by the OFA and IS&S.

7. Use of third party website: All departments that accept cards over the internet through any means (including phone applications and mobile solutions), must redirect all such card submissions to a third party website authorized and approved in writing by the OFA and IS&S.

8. Closing merchant account: Closing merchant accounts is the sole responsibility of the OFA in accordance with this section. A department that wishes to close a merchant account must request this in writing to the OFA, representing, as applicable, that:

a) The department is the business owner of the merchant account to be closed;
b) All terminal equipment has been returned to the OFA;
c) All e-commerce activity has been decommissioned; and
d) Any paper or electronic records will be destroyed in accordance with the College's record management policy.

Upon confirmation, the OFA will arrange for the merchant account to be closed.

Appendix C Business Standards

The school or department must have procedures to ensure the following:

1. Card processors do not accept card transactions for more than the amount of purchase and the amount entered into the card machine agrees with the purchase amount.

2. The card expiration date is not included on the receipt.

3. Only the last 4 digits of the card number prints on the receipt copy given to the customer.

4. Card data will not be stored absent a legitimate business purpose as approved by the OFA. In no event will CVV, PIN or expiration date be stored.

5. Hard copies of card data, if any, will be stored with appropriate physical safeguards, including storage in locked cabinets with access restricted to those with legitimate business need.

6. Electronic copies of card data, if any, will be stored with appropriate technical safeguards as approved by the OFA and IS&S.

7. If a client workstation becomes impaired or inoperable, cards must only be processed in a PCI compliant alternative process.