CREDIT CARD SECURITY POLICY – PCI DSS 2.0

Introduction and Scope

Introduction
This document explains Buena Vista University’s credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. Buena Vista University management is committed to these security policies to protect information utilized by Buena Vista University in attaining its business goals. All employees are required to adhere to the policies described within this document.

Scope of Compliance

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, Buena Vista University’s cardholder environment consists only of imprint machines or standalone dial-out terminals. The environment does not include storage of cardholder data on any computer system.

Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) B, ver. 2.0, October, 2010. Should Buena Vista University implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ B, it will be the responsibility of Buena Vista University to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Protect Stored Cardholder Data

Prohibited Data
Processes must be in place to securely delete sensitive authentication data post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)

Payment systems must adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):

- The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)
- The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)
• The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. 
  (PCI Requirement 3.2.3)

Displaying PAN

Buena Vista University will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show only the first six and the last four digits of the PAN. (PCI requirement 3.3)

Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to Buena Vista University’s cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

• Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.1)

• Privileges must be assigned to individuals based on job classification and function (also called “role-based access control”). (PCI Requirement 7.1.2)

Restrict Physical Access to Cardholder Data

Physically Secure all Media Containing Cardholder Data

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI requirement 9.6)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include:

• Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.7.1)

• Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.7.2)

Logs must be maintained to track all media that is moved from a secured area, and management approval must be obtained prior to moving the media. (PCI Requirement 9.8)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.9)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.10)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. Container storing information waiting to be destroyed must be secured to prevent access to the contents. (PCI requirement 9.10.1)

Maintain a Policy that Addresses Information Security for Employees and Contractors
Security Policy

Buena Vista University shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data. (PCI Requirement 12.1)

This policy will be reviewed two months prior to the expiration date of BVU’s PCI compliance attestation each year. At this time the University Compliance Coordinator shall distribute the existing policy to President’s Council and the Incident Response Team for review and/or changes and any updates will be made prior to BVU’s PCI compliance attestation date. If it is determined that this policy must be updated to reflect changes to business objectives or the risk environment prior to this deadline, the University Compliance Coordinator will coordinate this activity. (PCI requirement 12.1.3)

Critical Technologies

Buena Vista University shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

These policies must include the following:

- Explicit approval by authorized parties to use the technologies (PCI Requirement 12.3.1)
- A list of all such devices and personnel with access (PCI Requirement 12.3.3)
- Acceptable uses of the technologies (PCI Requirement 12.3.5)

To address these requirements, the following procedures and best practices shall be required for all critical employee-facing technologies:

- Explicit management approval for device use
- All device use shall be authenticated were feasible with username and password or other authentication item (e.g. token)
- An inventory shall be maintained for all devices and personnel authorized to use the devices
- Labeling of devices to facilitate tracking of owner, contact information, and purpose
- Automatic disconnect of remote access sessions after a specific period of inactivity
- On-demand activation of remote access solutions used by vendors only when needed, with immediate deactivation after use

Additionally, personnel shall be kept informed of the following:

- Acceptable uses for the technology
- Acceptable locations for use of the technology
- Prohibition of the storage of cardholder data onto local hard drives or other external

Security Responsibilities

Buena Vista University’s policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

In accordance with this requirement, the following responsibilities have been established:

1. The Presidents Council is the final authority for the institution’s governance of information security policy and procedure, including:
   - Approval of all policy specific to information security
   - Approval of all actions taken in response to any suspected or real security incidents

2. The Chief Information Officer is responsible for overseeing all aspects of information security, including but not limited to the following:
• Creating and distributing security policies and procedures
• Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel
• Periodic analysis, identification, and ranking of emerging security vulnerabilities
• Review security logs and follow-up on exceptions

3. The University Security Incident Response Team shall establish, document, and distribute security incident response and escalation procedures (Incident Response Plan) to ensure timely and effective handling of all situations, including:
   • Roles, responsibilities, and communication
   • Coverage and responses for all critical system components
   • Notification, at a minimum, of credit card associations and acquirers
   • Strategy for business continuity post compromise
   • Reference or inclusion of incident response procedures from card associations
   • Analysis of legal requirements for reporting compromises
   • Annual testing
   • Designation of personnel to monitor for intrusion detection, intrusion prevention, and file integrity monitoring alerts on a 24/7 basis
   • Plans for periodic training
   • A process for evolving the incident response plan according to lessons learned and in response to industry developments

The membership of the University Security Incident Response Team shall be comprised of the following University personnel:
• VP of Business Services
• VP of Student Affairs
• VP for Academic Affairs and Dean of the Faculty
• University Compliance Coordinator
• Chief Information Officer
• Chief Technology Officer
• Assistant Director of Information Technology
• Director of Campus Security
• Director of University Marketing & Communications
• Manager of Human Resources
• University General Counsel

4. The University Compliance Coordinator is responsible for coordinating the following compliance-related activities:
   • Liaison with credit card associations and acquirers on matters specific to PCI compliance
   • Coordination of the annual PCI attestation process, including:
     o Distribution of University Credit Card policy to stakeholders for review
Collecting and compiling any policy updates for final review and approval
Posting and communication of policy updates to the community at large
Conducting and submitting the on-line attestation questionnaire

- Alert the President or daily designee of received incident reports
- Coordination and scheduling of activities involving the University Security Incident Response Team
- Maintaining a formal security awareness program for all employees that provides multiple methods of communicating awareness and educating employees (for example, posters, letters, meetings)

5. The Information Technology Department shall maintain daily administrative and technical operational security procedures that are consistent with the PCI-DSS. System and Application Administrators shall perform the following roles:

- Establish and adhere to a change control policy and process for all changes to system components
- Perform periodic system component security testing
- Monitor and analyze security alerts and information and distribute to appropriate personnel
- Administer user accounts and manage authentication
- Monitor and control all access to critical data
- Retain audit logs in accordance with institution retention policy
- Develop software applications in accordance with PCI-DSS and based on industry best practices

6. Faculty-staff manager/supervisors are responsible for ensuring that the activities under their direction adhere to these policies and that employees participate in security awareness programs:

- Ensuring that employees have read and understand the university’s information security policies
- Screen potential employees to minimize the risk of compromise or exploit from within the organization

7. Internal Audit (or equivalent) is responsible for executing a risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.

8. The General Counsel’s Office will ensure that for service providers with whom cardholder information is shared the following practices are observed:

- Contracts require adherence to PCI-DSS by the service provider
- Contracts include written acknowledgement or responsibility for the security of cardholder data by the service provider

Incident Response Policy

The University Security Incident Response Team shall establish, document, and distribute security incident response and escalation procedures (Incident Response Plan) to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to:

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/authorized physical entry)
- Fraud – Inaccurate information within databases, logs, files or paper records
Reporting an Incident

The University Compliance Coordinator should be notified immediately of any suspected or real security incidents involving cardholder data:

- Contact the University Compliance Coordinator to report any suspected or actual incidents. The Internal Audit’s phone number should be well known to all employees and should page someone during non-business hours.
- No one should communicate with anyone outside of their supervisor(s) or members of the University Security Incident Response Team about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the University Compliance Coordinator with the Directors of both Campus Security and University Marketing & Communications under the direction of the Vice President of Business Services with final approval of Presidents Council.
- Document any information you know while waiting for the University Compliance Coordinator to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.
- In response to a received report, the University Compliance Officer shall alert the President or, if absent, the person in charge for the day. It shall then be the decision of the President or daily designee to convene the University Security Incident Response Team.

Incident Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.
   - Visa
     Provides the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa’s “What to do if compromised” documentation for additional activities that must be performed. That documentation can be found at http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf
   - MasterCard
   - Discover Card
     Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

2. Alert all necessary parties. Be sure to notify:
   a. Merchant bank
   b. Local FBI Office
   c. U.S. Secret Service (if Visa payment data is compromised)
   d. Local authorities (if appropriate)
3. Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used:

   http://www.ncsl.org/programs/lis/cip/priv/breach.htm

4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Chief Information Officer will work with legal and management to identify appropriate forensic specialists.

5. Eliminate the intruder's means of access and any related vulnerabilities.

6. Research potential risks related to or damage caused by intrusion method used.

**Root Cause Analysis and Lessons Learned**

Not more than one week following the incident, members of the University Security Incident Response Team and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

**Security Awareness**

Buena Vista University shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. *(PCI Requirement 12.6)*

**Service Providers**

Buena Vista University shall implement and maintain policies and procedures to manage service providers (if cardholder data is shared). *(PCI requirement 12.8)*

This process must include the following:

- Maintain a list of service providers *(PCI requirement 12.8.1)*
- Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess *(PCI requirement 12.8.2)*
- Implement a process to perform proper due diligence prior to engaging a service provider *(PCI requirement 12.8.3)*
  - Monitor service providers’ PCI DSS compliance status *(PCI requirement 12.8.4)*
## Revision History

<table>
<thead>
<tr>
<th>Changes</th>
<th>Approval</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td>President's Council</td>
<td>9/10/2012</td>
</tr>
<tr>
<td>Further clarification and definition of Critical Technologies, Security</td>
<td>President's Council</td>
<td>10/29/2012</td>
</tr>
<tr>
<td>Responsibilities, and Incident Response</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>