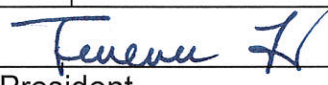


BBCC ADMINISTRATIVE PROCESS

Title: Credit Card Security Procedure	AP 8045	Implementing Board Policy: 8045
Originating Department: Business Office	Originated:	Effective Date: 5/8/15
Previous Revisions:	Approved: 	President

1.0 PURPOSE

The Payment Card Industry Data Security Standard (PCI DSS), a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis. PCI DSS compliance is mandatory for any organization that collects, processes, or stores credit card information.

The purpose of this procedure is to establish requirements for collecting, storing, processing, and transmitting credit card data to facilitate compliance with the PCI DSS requirement.

Cardholder Data/Payment Card Data is all personally identifiable data about the cardholder (i.e. account number, expiration date, data provided by the cardholder, other electronic data gathered by the merchant/agent, etc.) This term also accounts for other personal insights gathered about the cardholder, i.e., addresses, telephone numbers, magnetic stripe data, and CVC2/CVV2.

2.0 AUTHORITY

Implementing Board Policy 8045, RCW 19.255.020 Liability of processors, businesses, and vendors Payment Card Industry Data Security Standard (PCI DSS).

3.0 SCOPE

This procedure applies to all Big Bend Community College employees, contractors, consultants, temporary workers, and other workers. This procedure is applicable to any unit that processes, transmits, or handles cardholder information in a physical or electronic format.

4.0 PROCEDURE

All individuals authorized to accept payment cards must securely process, store, and dispose of payment card data (paper and electronic media) in order to adhere to the Payment Card Industry Data Security Standards (PCI DSS).

- 4.1 No electronic credit card numbers should be transmitted or stored in any other system, personal, computer, or email account.
- 4.2 Physical cardholder data must be locked in a secure area and limited to only those individuals that require access to the data. In addition, restrict access to data on a "need-to-know" basis.
- 4.3 Stored credit card information will be retained for a maximum of 60 days. All media used for credit cards must be destroyed when retired from use. All hardcopy must be shredded prior to disposal.
- 4.4 Access to physically stored cardholder data is restricted and available only to Business Office employees whose job requires access to such information.

5.0 PROCEDURE

Big Bend Community College employees are governed by various policies that include the Code of Conduct, Acceptable Use, Information Security policies, the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach Bliley Act (GLBA), and the Red Flag Policy. These policies include the responsibility to protect the confidentiality of individuals' personal information. Big Bend Community College will conduct an annual security assessment per the guidelines of PCI DSS.

All credit card and debit card transactions, including web-based procurement of the same, must be initiated and controlled through the Business Office. The practice of least privilege will be utilized to restrict access to sensitive data. This practice involves assigning individual access on a "need-to-know" basis. For employees without a "need-to-know," credit card account numbers will be masked to protect account information.

Under no circumstances will it be permissible to obtain credit card information or transmit credit card information by email. If an email containing cardholder data is received, it must be immediately deleted and the sender must be notified that Big Bend Community College does not accept cardholder data via email and that the transaction will not be processed.

6.0 DATA STORAGE AND DESTUCTION

The following processes must be followed for all data storage and destruction:

- 6.1 When destroying physically stored credit card information, hard copy of cardholder data is cross-shredded by an employee before it is disposed so that data cannot be reconstructed.
- 6.2 All electronic media containing cardholder information should be labeled and identified as confidential.

7.0 SANCTIONS

Failure to meet the requirements outlined in this policy may result in suspension of physical and/or electronic payment capability for affected units. Additionally, the credit card associations may impose fines. Persons in violation of this policy are subject to the

full range of sanctions, including the loss of computer or network access privileges, disciplinary action, suspension, termination of employment and legal action. Some violations may constitute criminal offenses under local, state, and federal laws. The College will carry out its responsibility to report such violations to the appropriate authorities.

