Becker's PCI Policy

OVERVIEW:

This policy addresses Payment Card Industry (PCI) Data Security Standards (DSS) that are contractually imposed by the major credit card brands on merchants that accept these cards as forms of payment.

APPLICABILITY:

The policy covers the following specific areas contained in the PCI standards related to cardholder data: collecting, processing, transmitting, storing and disposing of cardholder data. All departments that participate in credit card processing must have documented procedures pertaining to the items noted above. The documents should be available for periodic review.

DEFINITIONS:

- Cardholder data – Any personally-identifiable data associated with a cardholder. Such data include account number, expiration date, name, address, social security number, Card Validation Code, Card Verification Value, Card Identification Number, or Card member ID.
- PCI-DSS - Payment Card Industry Data Security Standards

ADMINISTRATION AND IMPLEMENTATION:

1 Credit Card Acceptance and Processing

1.1 In the course of doing business at Becker College, it may be necessary for a department to accept credit cards for payment. The opening of a new merchant account for the purpose of accepting and processing credit cards at the College is done on a case by case basis and coordinated through the Controller and CFO.

1.2 Any department accepting credit cards on behalf of the College must designate an individual within the department who will have primary authority and responsibility within that department for credit card transactions.

1.3 Specific details regarding processing and reconciliation will depend upon the method of credit card acceptance and type of merchant account. Detailed instructions will be provided by the Controller when a new merchant account is opened.

1.4 On a quarterly basis, the Assistant Vice President for Administration will inspect all credit card devices on campus to ensure they have not been tampered with. This includes looking for unexpected attachments or cables plugged into the device, looking for missing or changed security labels, looking for broken or differently colored casing, or looking for changes to the serial number or other external markings.

2 Credit Card Data Security Policy

Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

2.1 Cardholder data collected are restricted only to those users who need the data to perform their jobs. Each department must maintain a current list of employees with access and review the list annually, or when there is a change in staff, to ensure that the list reflects the most current access needed and granted.

2.2 Cardholder data, whether collected on paper or electronically, are protected against unauthorized access.

2.3 All equipment used to collect data is secured against unauthorized use in accordance with the PCI Data Security Standard.

2.4 Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents or electronic files containing cardholder data.

2.5 PCI Compliance at Becker is a joint effort. There are several areas affected by PCI including Student Accounts and Advancement. The Chief Information Officers will work with departments that process credit cards to ensure that the departments are PCI compliant. Individual departments are held responsible for PCI compliance for all departmental procedures, applications, point of sale devices and departmentally administered servers that process, store or transmit cardholder data.

2.6 E-mail should not be used to transmit credit card or personal payment information, nor should it be accepted as a method to supply such information. In the event that it does occur, disposal as outlined in #2.10 below.

2.7 If a fax machine is regularly used to transmit credit card information to a merchant department, that machine should be a stand-alone machine with appropriate physical security. Disposal of credit card information provided via fax should follow #2.10 below.

2.8 No database, electronic file, or other electronic repository of information will store full credit/debit card numbers, the full contents of any track from the magnetic stripe, or the card-validation code.

2.9 Becker issued computers and portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: desktops, laptops, compact disks, floppy disks, USB flash drives, personal digital assistants and portable external hard drives.

2.10 Cardholder data in paper form should be retained for three months or less for reconciliation purposes and destroyed immediately following the required retention period. A regular schedule of deleting or destroying data should be established in the department to ensure that no cardholder data is kept beyond the record retention requirements. Paper documents should be shredded in a cross-cut shredder. Electronic data should be sanitized with an electronic shredding tool sponsored by the College.

3 Responding to a Security Breach

In the event of a breach or suspected breach of security, the department or unit must immediately execute each of the relevant steps below:

3.1 Document every action you take from the point of suspected breach forward, preserving any logs or electronic evidence available.

3.2 If the affected machine is a desktop or laptop, disconnect the computer/devices(s) from the network. To disconnect the device from the network, simply unplug the Ethernet (network) cable, or if the computer uses a wireless connection, disconnect from the wireless network. If the affected device is a server, contact the Chief information Officer or the Technical Director and ask to disconnect the device from the Network. DO NOT turn the computer device off or reboot. Leave the device powered on and disconnected from the network.

3.3 Notify the Chief Information Officer and the Director or department head of the department experiencing the breach. Email (from an unaffected system) may be used for initial contact but the details of the breach should not be disclosed in email correspondence.

3.4 Prevent any further access to or alteration of the compromised system(s). (i.e. do not log on to the machine and/or change passwords; do not run a virus scan). In short, leave the system(s) alone, disconnected from the network, and wait to hear from a security consultant.

3.5 If warranted, Becker will invoke its Data Breach Response Plan with further notifications and procedures.

ENFORCEMENT:

Failure to meet the requirements outlined in this policy may result in suspension of the physical and, if appropriate, electronic payment capability with credit cards for affected departments. Any person that violates this policy will be subject to the same disciplinary actions as outlined in Becker's Confidentiality Agreement.

APPROVAL:

Approved by Becker's Information Security Advisory Committee on November 14, 2011.

REVIEW CYCLE:

This program will be reviewed and updated as needed, at least annually, based on the recommendations of the Chief Information Officer and Chief Financial Officer.