ADM 411
Security Policy #11
PCI DSS for Accepting Credit Card Payments Policy

Purpose of Policy

In order to accept credit card payments, the College is required to comply with the Payment Card Industry Data Security Standards (PCI DSS), which were established by a group of credit card companies (American Express, Discover, JCB, MasterCard, Visa) to protect merchants and cardholders from cardholder information theft. The College must also comply with the Federal Trade Commission's Fair and Accurate Credit Transactions Act (FACTA), which was also intended to reduce identity theft. This policy will be reviewed at least annually and will be updated as needed to reflect changes to the business objectives or the risk environment.

Policy

In order to comply with these standards and to provide adequate data security measures, Departments must contact the Business Office to receive approval prior to accepting credit cards information and follow the procedures described below to ensure the security of credit card information. Departments will need to consider the impact of credit card fees and note that most merchant service agreements prohibit or enforce strict rules regarding the assessing of convenience fees and surcharges to the consumer.

Departments are prohibited from collecting credit card information on the McPherson College network, storing any credit card information electronically, or sending credit card information via electronic means (e.g. email, chat, instant messaging). Devices used to process credit cards should use only the necessary services of the device to process credit card payments. All services not directly needed to perform the device's specified function should be disabled. These devices should only be used in locations where credit card acceptance is necessary and all procedures in this policy can be followed.

Access to cardholder data should be limited to only those individuals whose jobs require such access. Each individual with access to cardholder data should have a unique user ID, when applicable. User ID's should not be shared with other individuals. Approval should be obtained from the appropriate parties (IIT, Business Office, Individual Departments, etc.) to use credit card processing technologies.

Procedures

The following procedures should be adhered to when processing payments:

For credit card payments over the internet:

1. We must use payment gateways that are PCI DSS compliant for receiving, transmitting and storing credit card data. The transaction information should be collected and securely stored by the payment gateway or processor, so there is no reason for credit card data to be collected or stored on McPherson College computers or network.
2. Departments should obtain from the payment gateway or processor only the information necessary to apply the payment (such as the name and amount). There should typically not be any reason to obtain files or print reports containing the credit card data. The full contents of any track data from the magnetic stripe, the card verification code and the PIN should not be stored under any circumstances. In the event of dispute or chargeback, we can research the transaction on the processor's website via secure login.
3. IT policies are required to be followed when accepting credit card payments and IT personnel should be contacted to discuss all specific PCI security issues.

For credit card payments where a card is present:

1. Credit card equipment must be capable of protecting stored data and encrypting transmitted credit card data. Imprint machines should not be used.
2. Credit card information must be truncated to the last 5 digits. The full card number should never be printed on anything, including the customer copy, our copy or batch reports. In the event of dispute or chargeback, we can research the transaction on the merchant account website via secure login.
3. Any signed slips or batch reports should be retained in a locked file or vault for 18 months, and then securely destroyed. They should never contain the full card number.

For credit card payments when the card is not present (via mail or phone):

1. Follow rules that apply to "when card is present" or using the secure payment gateway.
2. Whenever possible, we should refer the individual to a secure payment gateway, rather than having them mail credit card information or writing it down over the phone. If it is absolutely necessary to have the credit card information in hardcopy, it should be entered promptly and then immediately destroyed by shredding so that cardholder data cannot be reconstructed. Containers storing information waiting to be destroyed must be secured to prevent access to the contents.
3. IIT policies are required to be followed when accepting credit card payments and IIT personnel should be contacted to discuss all specific PCI security issues.

The following procedures should be adhered to when setting up a credit card account:

1. Always contact the Controller or VP for Finance in the Business Office before setting up an account. In some cases, IT will also be contacted if it involves processing transactions via the internet. Departments and individuals processing credit card payments must sit down with the Business Office to be trained in the policies and procedures of accepting credit cards prior to accepting this type of payment.

2. The Business Office will set up each department merchant account under McPherson College's main headquarter account, which will enable the Business Office to access all accounts and research items when reconciling.
3. Separate merchant accounts should **not** be set up for Discover. Merchants now have the capability to clear Visa, MasterCard, and Discover together on a single merchant account. American Express has this capability as well, but the fees are higher for it, so we have typically set up separate American Express merchant accounts.
4. Departments should set their accounts up to deposit gross sales daily. Any fees should be debited out of the bank account as a separate transaction. Please do not set up the accounts to have fees net out of the sales deposit.
5. Departments must provide daily accounting records to the Business Office for credit card transactions, unless other arrangements have been made for the Business Office to import credit card deposit information from the payment gateways.
6. Access to credit card information should be limited to only those employees who need the information for their jobs and who deal with similar administrative duties on a regular basis.

The following procedures should be adhered to regarding 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. PCI DSS procedures must be followed to make sure college is PCI compliant. This must be reviewed at least once a year. 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 public safety, evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – Inaccurate information within databases, logs, files or paper records

The Controller or VP for Finance or security officer should be notified immediately of any suspected or real security incidents involving cardholder data. If you do not feel comfortable doing so, report your concern anonymously to the Campus Hotline at (866) 943-5787.

In the event that credit card information is compromised, the incident response steps under the **Security Incident Response #3** must be followed.

Also see **Appendix G - MC Trustwave - Credit Card Security Procedures.doc.**