Information Security Policy for
Presbyterian College Merchant Accounts

Ethics and Acceptable Use Policies

The College expects that all employees conduct themselves in a professional and ethical manner. An employee should not conduct business that is unethical or illegal in any way, nor should an employee influence other employees to act unethically or illegally. Furthermore, an employee should report any dishonest activities or damaging conduct to an appropriate supervisor.

Security of College information is extremely important. We are trusted by our student/constituents to protect sensitive information that may be supplied while conducting business. Sensitive information is defined as any personal data (i.e. name, address, phone number, Social Security number, driver's license number, bank account, credit card numbers, etc.) or College information not publicly available (i.e. financial information, employee information, schedules, technology, etc.). It is important the employees do not reveal sensitive information about our College or our constituents to outside resources that do not have a need to know such information.

Disciplinary Action

An employee's failure to comply with the standards and policies set forth in this document may result in disciplinary action up to and including termination of employment.

Protect Stored Data

Protect sensitive information stored or handled by the College and its employees. All sensitive information must be stored securely and disposed of in a secure manner when no longer needed for business reasons. Any media (i.e. paper, CD, backup tape, computer hard drive, etc.) that contains sensitive information must be protected against unauthorized access. Media no longer needed must be destroyed in such a manner to render sensitive data irrecoverable (i.e. shredding, degaussing, disassembly, etc.).

Credit Card Information Handling Specifics

- Destroy cardholder information in a secure method when no longer needed. Media containing card information must be destroyed by shredding or other means of physical destruction that would render the data irrecoverable (shred, degauss, etc.).

- Do not store the contents of the credit card magnetic stripe (track data) on any media whatsoever.
- Do not store the card-validation code (3 or 4 digit value printed on the signature panel of the card) on any media whatsoever.
- All but the last 4 numbers of the credit card account number must be masked (i.e. x's or *'s) when the number is displayed electronically or on paper.

Protect Data in Transit

If sensitive information needs to be transported physically or electronically, it must be protected while in transit (i.e. to a secure storage facility or across the internet).

Credit Card Information Handling Specifics

- Credit card account numbers must never be emailed without using proper encryption technologies (i.e. PHP encryption)
- Media containing credit card account numbers must only be given to trusted persons for transport to off-site locations.

Restrict Access to Data

Restrict access to sensitive information to those that have a need-to-know. No employees should have access to credit card account numbers unless they have a specific job function that requires such access.

Physical Security

Restrict physical security to sensitive information or systems that house that information (i.e. computers or filing cabinets storing cardholder data), to protect it from those who do not have a need to access that information.

- Media containing sensitive information must be securely handled and distributed.
- Media containing stored sensitive information (especially credit card account numbers and Social Security numbers) should be properly inventoried and disposed of when no longer needed for business by deleting, shredding, or degaussing before disposal.

- Password protected screen savers or Window's "Lock Computer" should always be used on any computers that may contain sensitive information.

Security Awareness and Procedures

Keeping sensitive information secure requires periodic training of employees to keep security awareness levels high. The following College policies and procedures address this issue:

- Hold periodic employee meetings to cover security awareness and training.
- Criminal background checks will be conducted for all new employees that handle sensitive information.
- All third parties with access to credit card account numbers are contractually obligated to comply with card association security standards (PCI/DSS).

Security Management / Incident Response Plan

The Director of Campus Police along with Business Office representatives is responsible for communicating security policies to employees and tracking the adherence to policies. In the event of a compromise of sensitive information, the Director of Campus Police will oversee the execution of the incident response plan.

Incident Response Plan

- If a compromise is suspected, alert the Director of Campus Police.
- The Director of Campus Police will conduct an initial investigation of the suspected compromise.
- If compromise of information is confirmed, the Director of Campus Police will alert management and begin informing parties that may be affected by the compromise. If the compromise involves credit card account numbers perform the following:
    - Contain and limit the extent of the exposure by shutting down any systems or processes involved in the compromise.
    - Alert necessary parties (Merchant bank, Visa Fraud Control, law enforcement).
    - Provide compromised or potentially compromised card numbers to Visa Fraud Control within 24 hours: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html