GRINNELL COLLEGE CREDIT CARD PROCESSING AND SECURITY POLICY

PURPOSE

The Payment Card Industry Data Security Standard was established by the credit card industry in response to an increase in identify theft and credit card fraud. PCI-DSS is a set of requirements designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment. As a merchant who handles credit card data Grinnell College is responsible for safeguarding credit card information and adhering to the standards established by the PCI-DSS. This includes establishing policy and setting up controls with regard to handling credit card data, computer and internet security related to credit card processing and annually completing a self-assessment questionnaire.

The purpose of this policy is to define requirements for accepting and processing payment cards in the course of College business that will protect customer's credit card data, uphold the College's reputation and minimize risk of financial costs associated with a breach of credit card information. Grinnell College requires that all departments that process, store or transmit credit card data remain in compliance the Payment Card Industry Data Security Standards at all times.

Penalties for not complying with the security requirements or failure to rectify a security issue may result in fines starting at $50,000 and/or restrictions on the merchant account. Consequences for non-compliance are severe. Therefore, Grinnell College mandates all departments and employees must comply.

DEFINITIONS

Cardholder Data

Cardholder Data represents any personal information of the cardholder. This may be an account number, expiration date, name, address, telephone number, social security number, card validation number (CVC), or any other identifying cardholder information.

Data Security Standards

Standards developed by the Payment Card Industry council that include controls for secure handling of sensitive consumer information to assure consumers their credit card brands are reliable and secure.

Merchant

An organization, department, institution or unit that accepts credit cards as a method of payment for goods, services, information, or gifts.

Merchant Account

An account established for a unit by a bank to credit sale amounts and debit processing fees.

Payment Card Industry (PCI)

A group formed by the credit card industry (Visa, MasterCard, Discover and American Express) to establish Data Security Standards (DSS) for the industry. https://www.pcisecuritystandards.org/

Self-Assessment Questionnaire

The SAQ is a validation tool that is primarily used by merchants to demonstrate PCI DSS compliance.

POLICY

1) Information Technology Services (ITS) is responsible for building and maintaining a secure network, including installing and maintaining a firewall configuration to protect data and assuring vendor-supplied passwords are changed prior to installing a system on the network. Information Technology Services will ensure that all router, switches, wireless access points and firewall configurations are properly secured.

2) Departments are prohibited from any electronic storage of cardholder data. All paper storage should contain only account numbers masked to display the last 4 digits of the account. Never store card validation code, expiration dates, PIN's, or full data from a card's magnetic stripe.

3) Information Technology Services will assure strong cryptography and security protocols are in place for transmission of cardholder data across open, public networks. Transmitting cardholder data by end-user technologies (ex: e-mail, instant messaging or chat) is prohibited.

4) Information Technology Services is responsible for maintaining a vulnerability management program that includes use and regular update of anti-virus software/programs and developing/maintaining secure systems and applications.

5) Access to cardholder data is restricted to those staff members who are responsible for processing or transmitting this data. Those staff members accessing card holder data electronically must have a unique password.

6) Paper copies of credit card data, retained for reconciliation purposes, must be store in the locked Accounting file room. Paper credit card data will be shredded each fiscal year once the annual audit has been completed. These paper copies are moved from Cashier to Accounting only by authorized Cashier or Accounting staff members. Departments are prohibited from transmitting credit card data by fax, e-mail, wireless network or unsealed envelopes through campus mail as these are not secure. Cardholder data should only be accepted by telephone, mail, or in person – never via email or transmitted on electronic forms. Paper documents on which cardholder data

has been written for processing must be shredded immediately after the transaction has been authorized by the credit card company. If it is necessary to hold this paperwork for a short period as it is processed it must be stored in a locked drawer in a locked office or file room.

7) Information Technology Services is responsible for regular testing of security systems and processes. This includes running internal vulnerability scans quarterly. External scans are performed by SecurityMetrics quarterly.

8) Accounting will provide training to ensure card processing departments are trained to accept and process credit card payments in compliance with Grinnell College's policy. This will include acquiring a signed confidentiality/non-disclosure statement from employees upon completion of training and testing.

9) Employees are prohibited from use of remote-access technologies, wireless technologies, any type of removable electronic media, laptops, personal data/digital assistants or email to transmit or process credit card data.

10) Grinnell College currently accepts American Express, Discover, MasterCard and VISA cards. Departments are authorized to accept only credit cards approved by the Controller. Any addition of merchant accounts or changes to existing merchant accounts must first be approved by the Controller. Purchasing, selling or discarding a terminal; purchasing software with any kind of credit card processing capabilities; or selecting/changing a service provider that has credit card processing capabilities must first be approved by the Controller. Contractual agreements with any third party vendor related to credit card processing must be approved by the Controller prior to signing the contract.

11) Every Grinnell College department accepting payment cards is subject to the Payment Card Industry Data Security Standards (PCI DSS).

12) Third party providers may not be used for any credit card processing until PCI compliance has been verified.

13) Accounting will verify annually that third party payment applications are compliant and, if applicable, on the Payment Application Best Practice (PABP) list.

14) Accounting and Information Technology Services will be responsible for reporting and for network security in the event there is a breach of cardholder data. This will include notifying the credit card company(s).

15) Information Technology Services will ensure that all router, switches, wireless access points and firewall configurations are property secured.

16) Information Technology Services will annually review their network security policy. Any updates will be shared with the Controller.

POLICY REVIEW

This security policy will be reviewed annually or as deemed necessary by the Treasurer's Office, given a specific event or change in the College's environment.

3/30/2011 mam

GRINNELL COLLEGE
CONFIDENTIALITY / NON-DISCLOSURE STATEMENT – CREDIT CARDS

As a Grinnell College staff member, I acknowledge that in the course of my employment I may have access to personal, proprietary, transaction-specific, and/or otherwise confidential data concerning faculty, staff, students, alumni and/or other persons through the processing of credit card transactions. As an individual with responsibility for transmitting, processing, and/or storing credit card data, I may have direct access to sensitive and confidential information in paper or electronic format. To protect the personal and proprietary data of those to whom Grinnell College provides service, along with protecting the integrity and the security of the systems and processes and to preserve and maximize the effectiveness of College resources, I agree to the following:

- I will maintain password confidentially by not disclosing passwords to others.
- I will utilize credit card data for College business purposes only.
- I have been provided a copy of Grinnell College's Payment Data Card Security Standard Policy regarding the proper processing, storing, protection and disposal of such confidential data. I will ensure that any such data is stored securely during the time the data is being processed and when the data is no longer needed for processing it is shredded or otherwise disposed of as per approved College policy and is.
- I have read, understand, and agree to abide by the PCI DSS Policy. Any violations to this Policy could result in disciplinary action.

Name (print)_____Signature_____Date_____

Department_____Supervisor_____Date_____