Golden Gate University Credit Card Security Policy

Effective Date: 2/1/2012

Approved by: [Signature]

I. PURPOSE
The purpose of this policy is to establish guidelines for processing charges/credits on credit cards to protect against exposure and possible theft of account and personal cardholder information that has been provided to Golden Gate University; and to comply with the Payment Card Industry's Data Security Standards (PCI) requirements for transferring, handling and storage of credit card information.

II. SCOPE
This policy applies to all Golden Gate University employees, contractors, consultants, temporaries, and other workers. This policy is applicable to any unit that processes, transmits, or handles cardholder information in a physical or electronic format.

III. POLICY
All transactions (including electronic based) that involve the transfer of credit card information must be performed on systems approved by the University's Finance Department, after a prior compliance and security review from Enterprise Technology Services (ETS). All specialized servers approved for this activity must be housed within ETS or an offsite hosting provider contracted by ETS and administered in accordance with the requirements of all Golden Gate University policies.

Golden Gate University is involved in PCI compliance and is subject to examination of system security and configuration to ensure cardholder information is securely maintained. The Finance Department will be responsible for verifying compliance with industry best practices for conducting electronic payment transactions through data capture/Point of Sale machines (credit card terminals), while web based procurement of credit cards will be monitored by ETS. In addition:

1. No electronic credit card numbers should be transmitted or stored in any other system, personal computer, handheld device, or e-mail account.
2. Physical cardholder data must be locked in a secure area, and limited to only those individuals that require access to that data. In addition, restrict access to data on a "need to know" basis.

3. Store only essential information. Do not store the card validation code or the PIN number. Do not store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.)

4. 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.

5. Departments must comply with the PCI Data Security Standard.

IV. PROCEDURES

Confidentiality and Security of Account Information
Golden Gate University 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 Rules Policy. These policies include the responsibility to protect the confidentiality of individual’s personal information.

All credit card & debit card transactions, including web based procurement of the same, must be initiated and controlled through the Finance Department. Because the sale of goods and services to entities outside the university community may raise special considerations (e.g. unrelated business tax, accounting, legal, etc) questionable sales should be reviewed by the Controller.

Departments who need to accept credit/debit cards and obtain a physical terminal to either swipe or key transactions through that data capture machine, need to contact the Finance Department to execute the required paperwork, obtain a Merchant Number, receive training, and be given direction as how to journalize those transactions on the books of the University.

Departments wishing to engage in electronic commerce are required to use a payment gateway approved by the Finance Department and ETS. A specialized Merchant Number will be established, and the department will be directed to the Chief Information Officer who will provide technical instructions and documentation.

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. Positions requiring specific levels of data access will be provided with approval by the department head, Controller, and the CIO. For employees without a "need to
know," credit card account numbers will be masked to protect account information. The last four digits are the maximum number of digits to be displayed.

Under no circumstances will it be permissible to obtain credit card information or transmit credit card information by e-mail or electronic messaging (IM) applications.

Under no circumstances will any other payment mechanism other than what has been approved by the CIO be permissible for electronic commerce on the web.

Any changes to systems housing account information must only be performed when:

- Thorough testing has taken place to ensure adequacies of controls;
- Functionality testing with clients has taken place;
- Required client training is completed;
- Change control processes have been followed.

Enforcement by Enterprise Technology Services

Chief Information Officer
- Responsible for monitoring the enforcement of this policy

Infrastructure and Operations Manager
- Responsible for coordinating activities around installation, modifications, and removal of all network hardware devices throughout Golden Gate University.

Applications Development Manager
- Responsible for coordinating activities around configuring the masking of account numbers based on a user's access.

System Administrators
- Responsible for granting permission to sensitive areas based on the principle of least privilege.

Data Storage and Destruction

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

- Hardcopy containing cardholder data will be destroyed immediately after processing.
- All electronic media containing cardholder information should be labeled and identified as confidential.
- An inventory of media containing cardholder information should be performed monthly.
- Audit logs for system housing cardholder data will be available for a period of four (4) years.
- Electronic backup media containing cardholder data will be available for a period of four (4) years and then properly erased or decommissioned and destroyed on a monthly basis.

V. SANCTIONS
Failure to meet the requirements outlined in this policy will result in suspension of physical and or electronic payment capability for affected units. Additionally, fines may be imposed by the affected credit card company, beginning at $50,000 for the first violation.

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 University will carry out its responsibility to report such violations to the appropriate authorities.

Violations of the policy will be addressed by the individual's respective disciplinary policies and procedures. All known and/or suspected violations must be reported to the applicable Network/System Administrator who will report, as appropriate, to the Chief Information Officer.

The appropriate University administrative office will investigate all such allegations of misuse with the assistance of Enterprise Technology services, Finance Department, and Human Resources.