Financial Officer

Date issued: May 1, 2015

Appendix A – PCI Security Safeguards

Any school or department that processes credit or debit cards agrees that it has implemented and will maintain the following security safeguards:

1. Credit card data is not stored in any format (e.g., electronic, hard copy) post-authorization absent written approval from Treasury Services. In no event are CVV, PIN and expiration data stored.

2. Hard copy materials containing credit card data (and approved by Treasury Services) have appropriate physical safeguards, including the following:

   - Credit card data is only retained for the minimum time necessary for its particular purpose;
   - Credit card data is stored in a secured and locked container (e.g., locker, cabinet, desk, storage bin) and access is restricted to those who are authorized to use the credit card data;
   - Credit card data is not removed from the premises; and
   - Credit card data is destroyed using a cross cut shredder when storage is no longer required.

3. All e-commerce transactions are processed through a third party hosted website approved by Treasury Services.

4. POS systems are segmented from other USC systems as confirmed by ITS Systems Security or its authorized delegate.

5. Workstations used to enter credit card transactions are segmented from other USC systems as confirmed by ITS Systems Security or its authorized delegate.

6. Stand-alone credit card terminals process through analog phone lines or wireless cellular connection and are not permitted to process over an internet connection absent written approval by Treasury Services.

7. Any technology used to access credit card data is authenticated via dual factor authentication as necessary, as determined by ITS Systems Security.

8. Cardholder data must be protected during transmission through the use of strong encryption. Cardholder data is not to be sent or received via email, instant messaging, or other end-user messaging technology.

9. All servers, workstations and mobile devices comply with the university's Network Infrastructure Use policy and the PCI standard, specifically regarding password management, access controls, anti-virus protection, patch management, audit log retention and physical security standards.

10. Mobile devices (laptops, iPads, thumb drives, etc.) are not permitted to process, store or transmit cardholder data absent written approval by Treasury Services.

11. All servers and workstations with access to cardholder data are scanned quarterly and findings are fully remediated. Audit logs are monitored on a regular basis and incidents addressed as required by the PCI Standard and USC policies.

12. All servers and third party systems that generate or transmit credit card data meet the USC hardening checklist requirements, as applicable.

13. Employees with access to credit card data are not permitted to directly access their workstations or laptops remotely without written approval from Treasury Services and in no event unless they use VPN or the Keckcare Portal.

14. Credit cards are not processed via USCNet.

Reviewed and approved by:

Signature of authorized representative (Dean, VP, CEO or authorized representative)	Signature of CTSS member
Print Name:	Print Name:
Date:	Date:

Appendix B – Procedures

1. Establishing merchant accounts**:** A school or department must obtain a merchant account from Treasury Services before accepting credit cards. A merchant account must be renewed annually. Before providing or approving a change to a merchant account, Treasury Services will require, as described below:
   a) A completed PCI Pre-Qualification form, as described in #2 below;
   b) Network diagram;
   c) Card flow diagram;
   d) Signed PCI Security Safeguards (Appendix A);
   e) Completion of PCI training by all USC employees who processes credit cards;
   f) Documentation supporting Third Party Vendor PCI compliance (see policy section on Third Party Vendor Risk Management); and
   g) Annual renewal requirements (see policy section on Annual Review).

2. PCI Pre-Qualification form: Any USC school or department that wants to accept credit cards must complete and submit a PCI Pre-Qualification form to Treasury Services. The form requires, among other things:
   a) A list of devices/methods and USC personnel by title authorized to use such devices/methods to process or otherwise access credit card information; and
   b) A legitimate business reason for the request to process credit card transactions.

The form also must be signed by the dean, director, vice president or CEO of the respective school or department, or authorized delegate, and the IT security liaison or authorized designee. Schools and departments may not begin to process credit cards until Treasury Services has given written approval.

3. School/department changes to how credit cards are processed**:** Schools and departments must submit to Treasury Services a revised pre-qualification, network diagram, card flow diagram and PCI Security Safeguards (Appendix A) form any time they propose to change the devices or methods used to process credit cards. Treasury Services must approve the change in writing before the school or department can implement the change. If a school or department is uncertain whether a particular change triggers this requirement, contact Treasury Services for guidance.

4. PCI Security Safeguards (Appendix A): Any USC school or department that wants to accept credit cards must agree to comply with the security criteria set forth in Appendix A. The PCI Security Safeguards must be renewed annually from the date of signature.

5. PCI training: All USC employees (including all faculty, staff, student workers and other employees) who handle credit card data must complete the university's PCI training program

before they will be permitted to access or process credit card data. In addition, training must be completed every fiscal year. As part of the annual training, employees handling credit card data must acknowledge that they have read and understand this policy. The school or department is responsible for maintaining a list of employees who handle credit card data and will provide it to Treasury Services, Compliance or Audit Services upon request. Treasury Services will provide training, maintain training records, and approve any exceptions in writing.

6. Use of authorized POS system: Any USC school or department that wants to accept credit cards through a point of sale ("POS") device or system must use a POS system authorized and approved in writing by Treasury Services.

7. Use of third party website: All schools or departments that accept credit cards over the internet through any means (including phone applications and mobile solutions), must redirect all such credit card submissions to a third party website authorized and approved in writing by Treasury Services.

8. Closing merchant account: Closing merchant accounts is the sole responsibility of Treasury Services in accordance with this section. A school or department that wishes to close a merchant account must request this in writing to Treasury Services, representing, as applicable, that:

a) The school or department is the business owner of the merchant account to be closed;
b) All terminal equipment has been returned to Treasury Services;
c) All e-commerce activity has been decommissioned; and
d) Any paper or electronic records will be destroyed in accordance with the university's record management policy.

Upon confirmation, Treasury Services will arrange for the merchant account to be closed.

Appendix C – PCI Incident Response Plan

All actual or suspected breaches must be reported to the Information Security Office (ISO) by calling (213) 740-5555, which is a call center operated 24 hours a day, 7 days a week. Upon notification, the ISO and Office of Compliance are responsible for investigating and coordinating with necessary members of the university community to ensure PCI requirements are met as described below. Departments may not conduct their own investigation without first consulting and coordinating with the ISO.

The ISO will:

- Determine whether an incident has occurred;
- Analyze and correlate initial information reported to the ISO;
- Gather research based on other means such as technical capabilities;
- If an incident is believed to have occurred, begin documenting the investigation and continue gathering evidence; and
- Ensure appropriate containment of the incident using the most appropriate options.

The ISO, in conjunction with the Office of Compliance, will:

- Prioritize handling the incident based on risk and impact to the organization; and
- Convene the incident response team described in this PCI policy, as applicable.

The Office of Compliance will:

- Engage IDExperts, as applicable, to facilitate call center and other consumer services;
- Conduct a legal analysis in coordination with Office of General Counsel to determine whether a breach has occurred as defined under law or regulations, including California Civil Code Section 1798.82; and
- Manage the breach notification process required under law or regulation.

The ISO and Office of Compliance will:

- Consult with the incident response team on a regular basis regarding the incident and status of response;
- Report to other units within USC and senior management based on the analysis of legal requirements and criticality of systems' information within USC's Business Continuity/Disaster Recovery Plans; and
- Implement appropriate corrective action, including administrative, physical and technical safeguards as recommended by the incident response team and approved by senior management.

The Office of Compliance will manage the process to report to appropriate parties in coordination with the ISO and incident response team:

- To the credit card issuing organizations to fulfill their PCI requirements:
  MasterCard
  http://www.mastercard.us/merchants/security/data-security-rules.html
  Visa
  http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html
  Discover
  http://www.discovernetwork.com/index.html - call fraud department at (800) 347-6634
  American Express
  https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US&tabbed=breach

- To local and federal law enforcement as deemed appropriate by the incident response team
- To impacted individuals
- To applicable state and federal regulatory agencies as required by law
- To Human Resources to determine appropriate disciplinary action, as applicable
- Implement additional monitoring to look for future related activity, if appropriate
- Prepare investigation report, as applicable

The incident response team will debrief from incident and implement any lessons learned.

Appendix D – Business Standards

The school or department must have procedures to ensure the following:

1. Credit card processors do not accept credit card transactions for more than the amount of purchase and the amount entered into the credit card machine agrees with the purchase amount.

2. The credit card expiration date is not included on the receipt.

3. Only the last 4 digits of the credit card number prints on the receipt copy given to the customer.

4. Credit card data will not be stored absent a legitimate business purpose as approved by the Office of Treasury Services. In no event will CVV, PIN or expiration date be stored.

5. Hard copies of credit card data, if any, will be stored with appropriate physical safeguards, including storage in locked cabinets with access restricted to those with legitimate business need.

6. Electronic copies of credit card data, if any, will be stored with appropriate technical safeguards as approved by Treasury Services and the ISO.

7. If a zero client workstation becomes impaired or inoperable, credit cards must only be processed in a PCI compliant alternative process, i.e. analog/wireless (CDMA) terminals or paper.