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: