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.