Appendix B

1. Establishing merchant accounts: A department must obtain a merchant account from University Financial Services and Treasury (UFS&T) before accepting credit cards. Before providing or approving a change to a merchant account, University Financial Services and Treasury will require, as described below:

a) A completed PCI Pre-Qualification form, as described in #2 below;

b) Signed PCI Security Safeguards (Appendix A);

c) Completion of PCI training by all WesternU employees who processes credit cards;

d) Documentation supporting Third Party Vendor PCI compliance (see policy section on Third Party Vendor Risk Management); and

2. PCI Pre-Qualification form: Any WesternU department that wants to accept credit cards must complete and submit a PCI Pre-Qualification form to UFS&T. The form requires, among other things:

a) The department's list of devices/methods and WesternU 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 director of the respective department, or authorized delegate, and the IT security liaison or authorized designee.

Departments may not begin to process credit cards until UFS&T has given written approval.

3. Department changes to how credit cards are processed: Departments must submit to UFS&T a revised pre-qualification and PCI Security Safeguards (Appendix A) form any time they propose to change the devices or methods used to process credit cards.

UFS&T must approve the change in writing before the department can implement the change. If a department is uncertain whether a particular change triggers this requirement, contact the financial accountant at UFS&T for guidance.

4. PCI Security Safeguards (Appendix A): Any WesternU 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 WesternU employees (including all faculties, 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, understand, and will comply with this policy and its related procedures. The individual department is responsible for maintaining a list of employees who handle credit card data and will provide it to University Financial Services and Treasury. UFS&T will provide training, maintain training records, and approve any exceptions in writing.

6. Use of authorized POS system: Any WesternU 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 UFS&T.

7. Use of third party website: All 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 UFS&T

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

a) The department is the business owner of the merchant account to be closed;

b) All terminal equipment must be returned to UFS&T within 30 days of closing the account;

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, UFS&T will arrange for the merchant account to be closed.