APPENDIX E

Information Security Agreement for Employees Processing Credit Cards

As a credit card handler or processor I agree to abide by the provisions in this document. If I need further clarification I will refer to the Wright State University Cash Collection and E-commerce Policy and Procedures located at: http://www.wright.edu/bursar/policies/cashcollections.html

I will NOT do the following:

1. Acquire or disclose any cardholder's credit card information without the cardholder's written consent including, but not limited to, the full or partial sixteen (16) digit credit card number, three (3) or four (4) digit validation code (usually on the back of credit cards), or PINs (personal identification numbers).
2. Transmit cardholder's credit card information by e-mail or fax.
3. Electronically store on a University computer file, server or other portable device such as a laptop, PDA, flash drive, etc. any credit card information.
4. Use an imprint machine to process credit card payments. (An imprint machine is a non-electronic portable device that slides over a customer's credit card and displays the full 16 digit credit card number on the customer copy.)
5. Share a computer password if I have access to web-based credit card processing.

I will DO the following:

1. At time of employment, agree to complete a background check within the limits of local law.
2. Change a vendor-supplied or default password if I have access to a computer with credit card processing.
3. Password-protect my credit card user account if I have access to online credit card processing.
4. Escort and supervise all visitors including WSU personnel in areas where cardholder information is maintained.
5. Store all physical documents or storage media containing credit card information in a locked drawer, locked file cabinet, or locked office.
6. Report immediately a credit card security incident to my supervisor, Computing and Telecommunications and the Office of the Bursar if I know or suspect credit card information has been exposed, stolen or misused. I will use the following methods to notify the appropriate parties:
    a. Supervisor- send email detailing the incident.*
    b. CaTS- complete and send online incident response form at:* https://www.wright.edu/cgi-bin/incidentresponse.cgi
    c. Bursar- send fax (937-775-5775 detailing the incident.*

*(This report must not disclose any credit card numbers, three or four digit validation codes, or PIN numbers. It must include a department name and contact number.)

Dept Name: _____ Employee Signature: _____

Date: _____ Print Name: _____