PAYMENT CARD SECURITY – ETHICS CERTIFICATION

I confirm that acting as an employee of the University of Florida, I will keep in strictest confidence all payment card information to which I have access in a manner pursuant to the enterprise wide UF Payment Card Policy and respective directives. I will also comply with all related policies issued by UF Information Technology and the UF Privacy Office.

I recognize that credit/debit card information is sensitive and valuable and that the University is contractually obligated to protect this information against its unauthorized use or disclosure in the manner defined by the Payment Card Industry Data Security Standard (PCI DSS). Should such information be disclosed to an unauthorized individual or organization, the University could be subject to fines, increased credit and debit card transaction fees and/or the suspension of all payment card privileges.

As an individual whose role may include the acceptance, storage, transmission and/or processing of credit/debit card information, I agree with the following statements:

- I understand that I may only accept credit and/or debit card payments using methods approved by Treasury Management's Payment Card Operations on behalf of the University Controller's Office.
- I understand that I must destroy credit and debit card information immediately following the transaction as described in the University of Florida Credit Card Standards.
- I understand that in cases where I suspect that a breach of credit or debit card information has occurred, I must immediately report the incident to the University's Privacy Office, as well as to Treasury Management's Payment Card Operations.
- I understand that it shall be a breach of ethical standards for any personnel of the University or third party with access to cardholder's personal information to divulge either directly or indirectly, any cardholder information.
- In compliance with University policy and the PCI DSS, I certify that I have successfully completed the appropriate training (TRM100 - PCI – Payment Card Security, or TRM150 - PCI for Front Line Staff) at hire and/or as required annually on a fiscal year basis.
- I commit to comply with all University policies and documented procedures with the understanding that failure to comply with the above requirements may subject me to a loss of credit card handling privileges and/or other disciplinary measures.
- I understand that students/guardians and other customers are not allowed to enter their credit card information on an employee's computer, or University owned payment processing device that is not approved by the Controller's office.

Merchant Name:_____ Merchant ID#:_____

Employee Name:_____ UFID: _____

Signature:_____ Date: _____

Return form to: Payment Card Operations, Treasury Management, PO BOX 112008. Please retain a copy for your records.