**Payment Card Merchant Manager Agreement**

W&M Payment Card Policy & Procedures defines the university’s policy and procedures to ensure that payment card information is accepted and handled securely to reduce the risk of identity theft and financial fraud to customers who make payments via such methods. The policy establishes the requirements departments must follow in the processing of payment card transactions to reduce risks inherently associated with the handling of payment card transactions. Besides ensuring you are trained in accepting, processing or reconciling payment card transactions, designated Merchant Managers are additionally responsible for ensuring their department is maintaining ongoing compliance with the Payment Card Industry (PCI) Data Security Standards (DSS). By annually signing this agreement you are committing to provide oversight to your department to ensure the following:

* Ensure departmental procedures and logs are created and maintained based on established guidelines.
* Ensure payment card activities comply with PCI DSS requirements and associated university procedures.
* Ensure all individuals involved with payment card transactions are aware of the importance of securing cardholder data.
* Ensure staff complete the annual trainings and agreements; Notify PCI Team of new staff.
* Report any suspected or confirmed breach
* Maintain an understanding and annually attest to the requirements as outlined in the Self Assessment Questionnaire(s) (SAQ)
* Notify PCI Team if I leave this position and/or a new Merchant Manager is designated

***By signing this document, I attest that I have read, understand and agree to comply with the conditions stated. I also attest to having reviewed the training and documentation appropriate to my position and responsibilities.***

Printed Name

Signature Date

Department

Supervisor Signature Date