UFF DIRECTIVE ON PCI/DSS COMPLIANCE

UFF is required to follow strict PCI requirements to protect donors’ and customers’ credit card data. PCI/DSS compliance is required of all merchants and service providers that store, process, or transmit cardholder data and applies to all payment channels, including retail, mail/telephone order, and e-commerce. The PCI/DSS are standards developed by the credit card industry to be followed by all merchants. These standards include controls for handling and restricting credit card information, computer and internet security, as well as the reporting of a credit card information breach.

UFF currently accepts VISA, MasterCard, Discover, Diners Club International, and American Express credit card payments as a convenience for its donors and customers, and has adopted and implemented policies and procedures designed to meet the compliance requirements of PCI/DSS.

It is the policy of UFF to meet all requirements prescribed by PCI/DSS, as set forth in UFF Policy on Credit Card Security Standards, or to implement acceptable variances as approved by the Qualified Security Advisor. To confirm compliance and meet the twelve requirements of the PCI DSS standards as noted below, UFF will complete the PCI Self-Assessment Questionnaire C (SAQ-C) and Attestation of Compliance annually.

High Level PCI/DSS Standards

Build and Maintain a Secure Network
  Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
  Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data
  Requirement 3: Protect stored cardholder data.
  Requirement 4: Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program
  Requirement 5: Use and regularly update anti-virus software or programs.
  Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures
  Requirement 7: Restrict access to cardholder data by business need-to-know.
  Requirement 8: Assign a unique ID to each person with computer access.
  Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks
  Requirement 10: Track and monitor all access to network resources and cardholder data.
  Requirement 11: Regularly test security systems and processes.
Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

Detailed requirements as set forth in the UFF Policy on Credit Card Security Standards are the main compliance requirements of PCI/DSS that are applicable to UFF. The applicable standard is referenced. The complete list of detailed requirements can be found on the PCI/DSS website at https://www.pcisecuritystandards.org.

Quarterly Requirements

UFF will have quarterly scans conducted by a certified Approved Scanning Vendor as required by the PCI/DSS Standards. (PCI 11.2)

Annual Requirements

UFF will complete the PCI Self-Assessment Questionnaire C (SAQ-C) and Attestation of Compliance annually and provide copies to the Qualified Security Advisor and merchant acquirer.

Approved Date: September 30, 2010

Leslie D. Bram, Associate Vice President

Revision history: Original version

Revised September 30, 2010