Payment Card Policies Glossary

This glossary defines certain terms utilized in the Fayetteville Policies and Procedures 309 Payment Card policy series. These definitions will periodically change as industry standards are modified.

Breach Notification Laws: Governing laws that require a merchant to notify customers of a data breach that results in loss or theft of that customer's Personally Identifiable Information (PII).

Business Continuity Plan (BCP): A documented plan for maintaining business operations in the event of a disaster or breach. A supplemental document will be provided by Credit Card Operations to detail the required elements of a Business Continuity Plan.

Cardholder Data Environment: The location where cardholder data is stored, processed, or transmitted.

Data Compromise: The exposure of sensitive or personally identifiable information (PII) resulting from either intentional security breach (an "attack") or human error.

Data Security Breach: The act of circumventing security controls on a system, thus allowing unauthorized access to data via an attack on the system. Data may or may not be compromised during a security breach.

Disaster Recovery Plan: A documented plan for Information Technology continuity in light of a disaster, emergency, or breach that details Incident Response testing procedures and data back-up procedures. A supplemental document will be provided by Credit Card Operations to detail the required elements of a Disaster Recovery plan.

Payment Card: Any credit, debit, or pre-paid credit/debit card. All payment card activity for the University of Arkansas is monitored by Credit Card Operations and Cash Management.

Payment Channel: The hardware/software used to conduct a payment transaction.

Personally Identifiable Information (PII): Information that can be used to uniquely identify, contact or locate an individual or that can be used in conjunction with other sources to uniquely identify an individual. In the case of payment card data, PII can be all printed and non-printed information contained on a payment card that identifies the customer. Credit Card Operations will identify and periodically update PII applicable to the 309 policy series, as revisions to industry regulations and other security factors require.

In the context of payment card operations, it is strictly prohibited for a University of Arkansas entity to retain the following elements of PII: Credit/Debit card number, Card Validation Code (CVC), customer's PIN, or contents of the magnetic stripe of a payment card.

PCI DSS: The Payment Card Industry Data Security Standard (hereafter referred to as the "PCI DSS") is the result of collaboration between the major credit card brands to develop a single approach to safeguarding sensitive data. The PCI DSS defines a series of requirements for handling, transmitting and storing sensitive data. Entities engaged in any form of payment card processing must comply with these standards as a condition of their payment card processing contracts. A copy of the PCI DSS can be obtained from Credit Card Operations.

Processing Method: The means by which authorized departments accept payment cards. Payment card transactions may only be accepted via walk-in (face-to-face) payment, telephone, or customer-initiated online payment. Tuition/Fee payments are accepted only as customer-initiated through the ISIS Student Center or Parent Portal. No department may accept a payment card transaction via mail, email, fax, or any end-user messaging technology, or on a website that collects payment card information unless the site is authorized by Credit Card Operations via a System Usage Waiver.

Risk Assessment: A documented process used to identify and qualitatively and/or quantitatively evaluate risks and their potential effects, including brand damage and monetary effects. A supplemental document will be provided by Credit Card Operations to detail the required elements of a Risk Assessment.

Server Data Environment: The location of a physical or virtual server machine used in the processing, transmitting or storing of cardholder data.

November 19, 2010