Payment Card Incident Response

Credit Card Operations will coordinate all responses to suspected or confirmed payment card security incidents. Payment card security incidents are defined as malicious attempts to access a payment system, successful attacks to compromise Personally Identifiable Information (PII), or any unauthorized access to a payment system, including internal access outside of an employee's job duties (even if accidental). Upon notification of a payment card security incident, Credit Card Operations will begin an immediate investigation into the reason for and scope of the incident. All processing for that payment acceptance channel will be suspended until after the investigation is completed and it is deemed safe to resume processing transactions.

The purpose of this policy is to establish procedures to evaluate, contain, and report any attempt to compromise the University of Arkansas online payment card system, QPay, or any alternate payment system authorized by Credit Card Operations. All incidents will be reported using the Credit Card Operations Incident Reporting System. False reporting of an incident is considered unlawful and appropriate disciplinary action will be taken.

Definitions

All terms mentioned in this policy are defined in the Payment Card Policies Glossary for the 309 policy series. All campus users of payment card information are required to know and fully understand all terms associated with the 309 policy series.

Department Responsibility

In the event of a payment card data security breach, the affected department is required to immediately notify Credit Card Operations via the *University of Arkansas Payment Card Incident Response System*, regardless of time of day. Training for designated incident response officers within each payment card processing department will be conducted annually by Credit Card Operations.

The affected department MUST discontinue processing transactions and disconnect all workstations, and/or POS systems from the University network. **DO NOT SHUT DOWN ANY EQUIPMENT**. All staff MUST remain logged-off of the affected systems. The department MUST not resume normal business operations until notified by Credit Card Operations. This requirement is enforced for ALL University of Arkansas departments, **regardless of the payment system used**. Credit Card Operations will coordinate all payment card security incident investigations for the University of Arkansas, including departments with an active System Usage Waiver.

If the breach is contained to one department, Credit Card Operations will assist that department with any required PCI DSS post-incident reporting. The department may be found to be responsible for any compromise, and processing privileges may be immediately revoked. Costs associated with the breach may be charged to the department if found to be negligent or in violation of the 309 policy series at the time of the breach.

Departments with an active System Usage Waiver MUST have their own Disaster Recovery, Business Continuity, and Risk Assessment policies and procedures in place. Those policies must be approved by Credit Card Operations prior to implementation. Credit Card Operations can assist departments in drafting and revising procedures as industry or processing environment changes occur. Departmental staff should immediately notify Credit Card Operations of a suspected compromise and Credit Card Operations will coordinate any and all investigations into an incident that results in a data breach to that system. If an incident occurs, all audit logging for the external processing system is to remain functional during and after an incident.

Credit Card Operations Responsibility

The Payment Card Industry Data Security Standard (PCI DSS) requires that the merchant MUST complete the following if a payment card data security breach is detected:

1. Immediately contain the exposure of the breach
2. Immediately notify the necessary institutional parties
3. Prepare the Incident Response Report and file with the merchant bank within 3 business days
4. Prepare a list of compromised accounts and file with the merchant bank within 10 business days

In the event of a payment card data security breach affecting the University of Arkansas online payment system, QPay will be taken off-line. Notice of disruption of service will be posted on the QPAYNEWS-L listserv. PCI DSS requires that the affected system be made unavailable until a forensic investigation is completed. Responses to incidents involving QPay will be governed by the QPay Disaster Recovery plan and be immediately executed by Credit Card Operations.

Credit Card Operations will assess the situation and will immediately begin notifying necessary parties of the incident as appropriate. Financial Affairs will make the determination whether the circumstances surrounding the incident require notification of law enforcement.

Annual testing of the University Incident Response plan is required to ensure all parties understand responsibilities for their area. During QPay Incident Response testing, QPay might be unavailable for transaction processing. The date/time of testing will be disseminated to all processing departments via the QPAYNEWS-L listserv. Departments with an active System Usage Waiver will also have their system tested as part of Credit Card Operation's annual Incident Response Plan testing.

November 19, 2010