Status Draft PolicyStat ID 15638452

Last Approved	N/A	Area	Finance (Procedures)
Effective	N/A	Chief Or Responsible Office	Business and Financial Services, Information Technology Services
Next Review	N/A		

Incident Response Plan

Authority for Procedure granted by UWG Policy 3003, Payment Card Industry Data Security Standards

An incident response plan is a requirement of the ~~Payment Card Industry Data Security Standards (PCI DSS)~~Payment Card Industry Data Security Standards (PCI DSS) to ensure that there is a systematic approach to addressing and managing the aftermath of a security incident. The objective is to handle ~~the situation~~situations in a manner that minimizes ~~the~~ recovery time and costs while determining corrective actions to mitigate future occurrences.

~~This procedure applies to all individuals that administer credit card payments for the University.~~

~~A. Scope~~

This procedure applies to all current UWG employees and/or volunteers that are involved in the acceptance of credit card payments for the University of West Georgia (UWG) and its affiliated foundations.

B. ~~For~~ Employees ~~That Are~~ Involved in an Incident

1. If an Incident is discovered during regular working hours (i.e. Monday - Friday; 8:00 a.m. to 5:00 p.m.), direct contact shall be made with one of the ~~following~~ PCI ~~Security Response Team~~Committee members ~~using the following sequence:~~

~~Information Security Officer~~	~~678.839.4007~~
~~PCI Compliance Analyst~~	~~678.839.2238~~
~~University Controller~~	~~678.839.5537~~
~~Deputy CIO~~	~~678-839-6100~~

~~PCI Committee Members~~	

.

2. If an Incident is discovered during evening hours (i.e. 5:00 p.m. – 8:00 a.m.), holidays, or weekends; direct contact shall be made with UWG Police at 678.839.6000.
    i. Upon answering a call regarding a credit card Incident, Police Dispatch shall notify one of the PCI ~~Security Response Team~~Committee members ~~according to the aforementioned sequence~~.
    ii. The team member that is contacted has the responsibility of notifying the remaining PCI Committee members.
3. ~~The team member that is contacted has the responsibility of notifying the remaining PCI Security Response Team members.~~
4. The PCI ~~Security Response Team~~Committee shall review the Incident and define the validity.
5. If an Incident is confirmed as a security risk, the PCI ~~Security Response Team~~Committee shall ensure that:
    i. The Incident is properly investigated and that the compromised department:
        a. minimizes the tampering of breached equipment;
        b. limits the exposure of cardholder data; and
        c. mitigates the risks associated with the Incident.
    ii. An independent PCI Forensic Investigator is contracted.
    iii. The appropriate acquiring bank must be notified.
    iv. All payment card brands that are utilized by the institution are notified.
    v. The institution's Information Security Officer shall notify the University System of Georgia {USG) cyber security representative.
    vi. The institution's insurance carrier is notified.
    vii. The appropriate credit card investigation report is completed and submitted to the affected credit card company.
    viii. Notification is provided to all pertinent University personnel (e.g. Chief Business Officer, President, Chief Information Officer, Chief ~~Communications~~Public Relations Officer, Chief of Police, Internal Audit, University Counsel, etc.)
6. Upon completion of the Incident response, the PCI ~~Security Response Team~~Committee will perform a "lessons learned" and "after-action review" of the Incident to determine factors contributing to the Incident and whether procedures and processes require amendments to avoid a similar Incident in the future.

C. Additional Resources

The University may engage the services of a consultant agency that provides guidance on an array of ~~PCIDSS~~PCI DSS issues. In the event of a breach, a ~~response team~~PCI Committee member shall notify the consultant for assistance.

A representative of the campus merchant that is impacted shall serve with the response team's investigation.

D. Compliance

The PCI Security Standards Council is a global open body formed to develop, enhance, disseminate, and assist with the understanding of security standards for payment account security. The Council was founded in 2006 by American Express, Discover, JCB International, MasterCard and Visa Inc. They share equally in governance and execution of the Council's work.

Note that enforcement of compliance with the PCI DSS and determination of any non-compliance penalties are carried out by the individual payment brands and not by the Council. Any questions in those areas should be directed to the payment brands.

Definitions

~~**Acquirer** - a financial institution that processes payment card transactions for merchants. Merchant Banks are subject to payment brand rules and procedures regarding merchant compliance (aka Acquirer, "acquiring bank," or "acquiring financial institution")~~

Cardholder Data - Any personally identifiable information associated with a person who owns a credit card.

~~**Compromised Data** - Account information of a cardholder that has been obtained by an unauthorized person.~~

Incident - Breach or attack whereby sensitive, protected, or confidential data has potentially been viewed, stolen, or used in an unauthorized manner.

~~**Merchant Bank** - For the purposes of this procedure, it has the same meaning as an Acquirer above,~~

~~**Payment Processor** - (aka "payment gateway", "payment service provider"). A third party engaged by the Merchant Bank to handle payment card transactions on their behalf. While Payment Processors typically provide acquiring services, they are not considered Acquirers unless defined as such by a payment card brand~~

PCI DSS – An acronym for Payment Card Industry Data Security Standards. The standards were established by the major credit card brands (i.e. Visa, MasterCard, American Express, Discover, and JCB) to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

~~**PCI Security Response Team**~~**PCI Committee** - Key University ~~personnel as identified by position in paragraph C.1 below~~employees who are responsible to investigate, evaluate, eradicate, communicate, and recover from payment card security Incidents while mitigating risks to the institution. The PCI Committee includes at a minimum the Assistant Director of Office of Student Accounts and Billing Services (OSABS), the Information Security Officer, and the Assistant Vice President (AVP) for Campus Services.

Approval Signatures

Step Description	Approver	Date