UNIVERSITY of West Georgia.

UWG PROCEDURE NUMBER: 5.3.1, PCI DSS Incident Response Plan
***Authority*: UWG POLICY: 5.3 (Payment Card Industry Data Security Standards)**

An incident response plan is a requirement of the 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 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.

The Chief Business Officer and the Chief Information Officer, pursuant to the authority of UWG Policy 5.3, establish the following procedures for compliance with PCI DSS standards for incident response.

A. Definitions

1. ***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")
2. ***Cardholder data*** – Any personally identifiable information associated with a person who owns a credit card.
3. ***Compromised data*** – Account information of a cardholder that has been obtained by an unauthorized person.
4. ***Incident*** – Breach or attack whereby sensitive, protected, or confidential data has potentially been viewed, stolen, or used in an unauthorized manner.
5. ***Merchant Bank*** – For the purposes of this procedure, it has the same meaning as an ***Acquirer*** above.
6. ***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
7. ***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.
8. ***PCI Security Response Team*** – Key University personnel as identified by position in paragraph C.1 below who are responsible to investigate, evaluate, eradicate, communicate, and recover from payment card security incidents while mitigating risks to the institution.

B. 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 and its affiliated foundations.

C. Procedures 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*** members using the following sequence:

1	Information Security Officer	678.839.4007
2	PCI Compliance Analyst	678.839.4781
3	University Controller	678.839.5353
4	Chief Information Officer	678.839.6100
5	Chief Business Officer	678.839.6410

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.
    a. Upon answering a call regarding a credit card ***Incident***, Police Dispatch shall notify one of the PCI Security Response Team members according to the aforementioned sequence.
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*** shall review the ***Incident*** and define the problem.
5. If an ***Incident*** is confirmed as a security risk, the ***PCI Security Response Team*** shall ensure that:
    a. The ***Incident*** is properly investigated and that the compromised department:
        i. minimizes the tampering of breached equipment;
        ii. limits the exposure of cardholder data; and
        iii. mitigates the risks associated with the incident.
    b. The appropriate credit card company is notified. Following are the telephone numbers for those credit card companies that are currently used at the institution:
        i. Visa – 1.650.432.2978
        ii. MasterCard - 1.800.999.0363 or Customer_Support@mastercard.com
    c. The appropriate merchant bank is notified. The telephone number for Bank of America is: 941.896.8881. Please check with the Controller's office for other banks, if applicable.
    d. The appropriate credit card investigation report is completed and submitted to the affected credit card company.
        i. For Visa, complete the **Visa Initial Investigation Report** – *click here*
        ii. For MasterCard, complete the **ADC Reporting Form** – *click here* for the manual; for the ADC Reporting Form, visit www.mastercardconnect.com.

e. Notification is provided to all pertinent University personnel (e.g. President, Chief Communications Officer, Chief of Police, University Counsel, etc.)

6. Upon completion of the ***Incident*** response, the ***PCI Security Response Team*** 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.

D. Additional Resources

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

E. 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.

Issued by the Chief Business Officer and Chief Information Officer, the 20th ***day of*** January, ***2017.***

_____ Signature,
Senior Vice President of Business and Finance

_____ Signature,
Vice President of Information Technology Services

Reviewed by President: _____

ADMINISTRATION & ADDITIONAL RESOURCES

Short Title: "PCI Policy" (UWG 5.3)

Previous Versions: N/A

Oversight: Chief Business Officer/Chief Information Officer

Additional Resources:

- Information Security Plan: http://www.westga.edu/assetsDept/infosec/UWG_IT_Security_Plan.pdf
- PCI: https://www.pcisecuritystandards.org/security_standards/index.php
- Institutional Guidelines for PCI Compliance: 5.3.2 http://www.westga.edu/assetsDept/pci/5.2.8._UWG_PCI_Procedures(2).pdf
- PCI Consultant – CampusGuard 402.408.6221 https://www.campusguard.com/