UWG Work Instruction: 5.3.1, PCI DSS Security Responsibilities

An integral component of PCI DSS is Requirement 12.1; the dissemination of security guidelines across all levels of the institution to ensure that a formal assessment is conducted, that compliance requirements are met, and that the guidelines are understood and reviewed on an annual basis.

The intent of this work instruction is to provide essential data security information to those personnel and supervision that are involved with the handling of credit/debit cards, credit/debit card data, and/or the systems that process such information for the University of West Georgia (UWG) and its affiliated foundations.

The PCI Security Response Team pursuant to the authority of UWG Policy 5.3, establish the following instructions for compliance with PCI DSS standards for a security event or incident response.

A. <u>Definitions</u>

1. ***Card verification value (CVV)*** **-** Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting
2. ***Cardholder data –*** Information that is associated with a credit/debit card – magnetic stripe, primary account number (PAN), cardholder name, expiration date, service code
3. ***Cardholder data environment*** **-** area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission.
4. ***Compliance Requirements*** – The formal act of obeying an order, rule, mandate, or request.
5. ***Encryption*** **-** Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.
6. ***Event –*** an outcome from a payment transaction that generates doubt, suspicion, or distrust. The event should be reported to a supervisor or a PCI Security Response Team member for further review.
7. ***Incident*** – Breach or attack whereby sensitive, protected, or confidential data has potentially been viewed, stolen, or used in an unauthorized manner.
8. ***Merchant*** – The department on campus that administers the payment transaction.
9. ***Payment device*** – Point of sales instrument that is used to transmit payment card data to merchant service provider for authorization and fund transfer. (aka Point of Sale terminal, credit card terminal, payment terminal, etc.)

10. ***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.
11. ***PCI Security Response Team*** – Key University personnel as identified by location of table in this document who are responsible to investigate, evaluate, eradicate, communicate, and recover from payment card security incidents while mitigating risks to the institution.

B. <u>Scope</u>

All personnel and supervision that are involved with the handling of credit/debit cards, credit/debit card data, and/or the payment devices and systems that process such information for the University of West Georgia (UWG) and its affiliated foundations

C. <u>Work Instructions for Employees and Supervision That Are Involved in Credit/Debit Card Payments</u>

1. All personnel and supervision that are involved with the handling of credit/debit cards, credit/debit card data, and/or the systems that process such information for the University of West Georgia (UWG) and its affiliated foundations must receive annual training in PCI DSS guidelines.
2. All personnel that are involved with administering a payment transaction (or supervise those that do) must understand that:
    a. additional training is required for understanding the payment device/system that is being used to process the transaction. Payment device information is incorporated with the area work instructions.
    b. cardholder data shall not be transmitted without an approved encryption solution.
    c. cardholder data that is transmitted shall be on devices and systems that are approved by the UWG PCI Security Response Team.
    d. credit/debit cards that are left or misplaced by customers in the vicinity of the transaction must be handed to the employee's supervisor. The supervisor is responsible for reporting this card to the appropriate credit card company and abide by that company's instructions.
        i. If the recommendation is to destroy the card, cut the card up in a manner that obliterates the account numbers.
        ii. If the recommendation is to hold the card until the customer is notified, secure the card in a locked storage area such as a safe.
    e. suspicious customer behavior shall be reported to supervision. If supervision is not available, contact UWG Police at 678-839-6000.
    f. compliance with the UWG PCI DSS policy, procedure, or work instruction is mandatory. Failure to follow these will be considered as gross misconduct and may result in disciplinary action, up to and including termination of employment.
3. Card holder data that is discovered on a computer, note book, phone message, copier, storage device, etc., shall be reported to the work area supervisor.
4. Prior to accepting a payment, the device/system that is being utilized shall be inspected for tampering. Examples of tampering include skimmers, damage, broken seal, false covers, etc. If tampering is suspected, the operator shall:

a. Cease using the device from operations for potential forensic inspection
b. Notify supervisor
c. Contact a PCI Security Response team member
d. Contact campus police

5. In rare instances, operations may be required to store cardholder data for a finite period of time not to exceed the close of the next business day. Approval for such data storage must be granted by the department head or designee.
   a. Storage of such information must be secured in a locked device during the day and an approved storage device overnight.
   b. Cardholder data is to be destroyed using a cross-cut shredder as soon as it has been transacted.
   c. Destruction of the cardholder data must be witnessed and documented by the employee's supervisor.
   d. Fax machines, POS devices and other equipment used for processing cardholder data must be in a secured cabinet or safe when not in use.
6. All personnel that are servicing payment devices and equipment should present their UWG credentials upon arrival. Consequently, personnel that are assigned to operate payment devices and equipment shall verify personnel credentials prior to servicing equipment.
   a. Any third party that is providing the service should be approved by supervision and accompanied by a UWG ITS representative.
   b. If payment device is replaced, UWG ITS representative is responsible for the appropriate documentation within equipment inventory.
7. If an outcome from a payment transaction generates doubt, suspicion, or distrust; the event should be reported to a supervisor for further investigation.
   a. The supervisor is responsible for notifying a member of the PCI Security Response Team using the prescribed sequence listed below:

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

   b. If an event or 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. Upon answering a call regarding a credit card event or incident, Police Dispatch shall notify one of the PCI Security Response Team members according to the prescribed call sequence.
   c. The PCI Response Team member is responsible for adhering to the security steps that are outlined in UWG Procedure 5.3.1.

D. Work Instructions for Employees and Supervision That Support the Cardholder Data Environment

1. All personnel responsible for technical support of the CDE and its infrastructure must receive annual PCI DSS and cybersecurity training.
2. All personnel providing service and support for CDE equipment must present appropriate credentials/identification when accessing merchant areas.
   a. Third parties that service and support CDE equipment must present their credentials upon arrival and have a member of the UWG ITS Division accompany them.
   b. UWG employees assigned to CDE service and support shall present their UWG credentials prior to servicing equipment.
3. Restrict access to physical network jacks, wireless access points, and routers.
4. Unless in use, switch and router ports will be disabled.
5. Maintain an inventory of network connecting devices as described in Table 1.
6. Maintain a list of network approval documents as described in Table 2.
7. Provide information by merchant areas regarding network components as described in Table 3.
8. Develop configuration standards for all system components and document them in Table 4.
9. Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). Record information in Table 5.
10. List employees that are responsible for security patch management using Table 6.
11. Document inventory of all system components directly associated with the CDE in Table 7.
12. Document resources for patch management, alerts, security and support in Table 8.
13. If applicable, provide information of outsourcing partnerships as described in Table 9.
14. Retain CDE audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).
15. Technical staff must insure that all cardholder data (CHD) and/or sensitive authentication data (SAD) are stored, transmitted, or processed in a secure manner within the CDE and supporting technical infrastructure.

E. Card Processing Environment Hardware Security

1. Technical staff shall implement and document firewall and router configuration standards that provide a:
   a. Formal process for approving and testing all network connections and changes to the firewall and router configurations
   b. Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks
   c. Current diagram that shows all cardholder data flows across systems and networks
2. Roles and responsibilities for logical management of network components shall be identified and documented. Roles include but not limited to:
   a. Security Admin,
   b. Network Admin,
   c. Approval admin, etc.
3. All services, protocols and ports allowed into and out of the CDE must be documented with a business need for use, and documentation must be provided for use of insecure protocols such as FTP, TFTP, Telnet, etc. including security measures afforded for their use.

4. General Configuration
    a. Disable all services not necessary for a business need specific to the CDE.
    b. Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.
    c. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).
5. System clocks on all equipment will be synchronized to a centralized time source located on the UWG Campus. Any exceptions must be approved by the ISO or CIO and documented.
6. All remote console access shall be encrypted using standard strong encryption techniques.
7. Configuration changes must be submitted to an authority for approval. Any changes must; be documented and dated, tested, and include rollback procedure.
8. Document all process and procedures defining discovery of new security vulnerabilities and update defined configuration standards accordingly.

1. Firewalls
    - Implement and maintain both an enterprise and host firewall solution that protects CDE networks and devices.
    - Firewall solutions must be configured:
        i. To DENY ALL incoming/outgoing traffic to/from the CDE networks and devices. Document all exceptions to the DENY ALL configuration explaining the specific business requirement(s) for exception(s).
        ii. To have default vendor passwords changed prior to installation on any network.
        iii. To disallow any direct traffic between the CDE and Internet.
        iv. Implement and maintain a formal change management process that documents any changes to firewalls supporting CDE networks and devices.
        v. Enable logging and log all incoming and outgoing connections related to the CDE, devices in the CDE, and devices supporting the CDE. Maintain log information for at least one year in a separate location.
        vi. Review firewall rule sets at least every six months and clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match the documented business justifications for the CDE networks and devices.

2. Network Equipment
    a. All networking equipment (switches, routers, IDS/IPS, etc.) will have default vendor passwords changed prior to being deployed.
    b. Document all connections to the CDE.
    c. Implement and maintain a formal change management process that documents any changes to CDE networks.
    d. Implement logging on all CDE related network equipment and maintain logged information in a separate location for at least a 1 year.
    e. Review firewall rule sets at least every six months and clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match the documented business justifications for the CDE networks and devices.

3. CDE Servers and Workstations
    a. Personnel implementing, deploying, maintaining, and supporting servers and workstations associated with CDE networks must employ prudent information security standards and best practices to minimize the risk and threats to the integrity, confidentiality, and availability of CDE networks and devices.
    b. Install only that software necessary for the operations of a CDE.
    c. When possible remove software not required for the CDE.
    d. When possible remove or disable unnecessary services from servers and workstations associated with the CDE.
    e. Employ host based firewalls to servers and workstations that deny all incoming traffic by default and will have exceptions for critical business functions only.
    f. Employ file integrity monitoring on all critical systems within the CDE.
    g. Set session idle time for servers and workstations to 15 minutes and require user to authenticate for restoring sessions.
    h. Protect access to the system BIOS via a password mechanism where available.
    i. Deploy antivirus/antimalware software capable of detecting, removing, and protecting against all known types of malicious software on all systems commonly affected by malicious software.
    j. Log all antivirus/antimalware activity.
    k. Servers participating in the CDE will have their security logs forwarded to a server external to the CDE.
    l. Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.

4. Vulnerability Assessments
    a. Vulnerability scans will be completed quarterly on all systems in the CDE. Urgent, critical or high vulnerabilities will be addressed immediately and systems re-scanned for complete remediation.
    b. External and internal penetration tests shall be completed annually and after any significant change to the infrastructure.

E. <u>Additional Resources</u>

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.

F. <u>Compliance</u>

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 PCI Compliance Analyst and Information Security Officer, the _____day of _____, 2017.

_____ Signature,
PCI Compliance Analyst

_____ Signature,
Information Security Officer

Reviewed by Vice President of Business and Finance _____

Reviewed by Vice President of Information Technology _____

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/

Table 1: Inventory of Network Connections Devices

Appliance	Brand	Model

Table 2: List of Network Approval Documents

Document	Name of Document	Main Purpose

Table 3: Network Component Roles and Responsibilities

Network Component	Name of Responsible Party and Title	Contact Email	Contact Phone Number	Group or Division within Organization	Roles and Requirements for Individual

Note: If your organization outsources the management and oversight of network connections and network devices to a third party outsourcing entity, then please use the following grid.

Table 4: Configuration Standards

System Component	Standard/Benchmark/ Framework Utilized	Date of Activity	Date of Completion	Name and Title of Individual

Table 5: Anti-Virus Attributes for the Cardholder Data Environment

Computers and System Components within Cardholder Data Environment that Utilize Anti-Virus	Anti-Virus Product Utilized	Current Version of Anti-Virus Product being Utilized	Virus Definition files Up To Date as Needed

Table 6: Security Patch Management Program Employee

Name	Title	Contact Information

Table 7: Inventory of All System Components Directly Associated with the CDE

System Components	System Name	Physical Location	Serial Number	Owner of System Components	Primary Use in Cardholder Data Environment

Table 8: Online Resources for Patch Management, Alerts, Security and Support

Vendor/Provider and Type of System	Website
CISCO	http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml
IBM AIX	http://www-03.ibm.com/systems/power/software/aix/service.html
Microsoft	http://technet.microsoft.com/en-us/wsus/default.aspx
Oracle	http://www.oracle.com/technology/deploy/security/alerts.htm
Apache	http://www.apache.org/dist/httpd/patches

Table 9: Outsourcing Partners

Network Component	Name of Responsible Outsourcing Party and Title	Contact Email	Contact Phone Number	Physical Mailing Address of Outsourcing Party	Roles and Requirements for Individual