BGSU®

Bowling Green State University

Payment Card Industry Data Security Standard

Information Security Policies

Table of Contents

Introduction

The Payment Card Industry (PCI) Security Standards Council, an organization composed of the major credit card companies, has developed data security standards to ensure that credit card transactions are reliable and secure.

Organizations that choose to accept credit card transactions as a form of payment are contractually required to follow the standards set forth by the PCI Security Standards Council. Failure to comply can result in more stringent requirements for compliance, fines, and/or suspension of credit card processing services.

The standards created include:

- **controls for handling and restricting credit card information**
- **computer and Internet security**
- **reporting of a breach of credit card information**

The credit card industry requires compliance with these standards in order for a merchant to accept credit card payments. Many departments and merchants on campus process credit card transactions in the course of daily business. As such, it is the intent of Bowling Green State University (BGSU) through this policy to protect the privacy of our customers and maintain compliance with *Payment Card Industry Data Security Standards* (PCI DSS).

This manual defines all policies and procedures required for compliance with the Payment Card Industry Data Security Standard (PCI DSS). These policies apply to all employees, systems and networks involved with credit card processing which includes; transmission, storage and/or processing of credit card numbers at Bowling Green State University

All employees involved in the Card Processing Environment (CPE) must read, understand and agree to abide by all policies in this manual. Any changes to the policies herein must be approved and disseminated by BGSU PCI DSS Compliance Committee.

These policies may be updated at anytime and must be reviewed annually for changes.

Not all components of the requirements listed in this document are directly applicable to the individual BGSU merchants, but are required to be attained by the BGSU as a whole. Questions regarding this policy should be directed to the BGSU PCI DSS Compliance Committee.

BGSU PCI DSS – General PCI DSS Policy

INTRODUCTION:

The following processes are for use by departments accepting credit cards as a form of payment in conducting official business at Bowling Green State University. BGSU accepts credit card payments as a convenience to its customers. Departments that have been approved to do so may accept VISA, MasterCard, Discover, American Express, debit cards with a VISA or MasterCard logo, and pin-based debit. Departments accepting credit cards at BGSU are required to follow strict procedures to protect customers' credit card data. Furthermore, these directives provide guidance to maximize compliance with the Payment Card Industry (PCI) Data Security Standards (DSS) and to ensure appropriate integration with the University's financial and other systems.

To become approved to accept credit cards, departments should contact the Treasury Department or Business Operations to discuss credit card processing options. Treasury and Business Operations must be included prior to purchasing credit card applications. Depending on the determined credit card processing type, a merchant ID may need to be established.

It is the policy of Bowling Green State University that only departments who have been approved may accept payment for goods or services via credit card. University departments will be held liable for all penalties resulting from non-compliance with this policy.

PROCESSING TYPES:

Point of Sale (POS)

Definition: The location where a credit card transaction occurs through a terminal or register.

Applicable Parties: Determined by a high frequency of business traditionally transacted through POS (register) devices, bank-owned desktop terminals and/or computers.

eCommerce

Definition: The buying and selling of products or services over the Internet.

Applicable Parties: Determined by a medium to high frequency of business traditionally transacted through web-based software. Transactions could occur through the centralized University provider or decentralized (department specific) BGSU-owned software.
Any e-commerce transactions at the University must be processed using the University's preferred provider *unless* an exception is approved by Treasury/Business Operations.

Third Party

Definition: Credit card transactions are processed through an external

party to BGSU. Software may or may not be owned by BGSU. Any new credit card processing application that is implemented after January 1, 2012 must be processed by a third party processor unless special permission is granted by Business Operations.

Applicable Parties: Determined by a medium to high frequency of business traditionally transacted through POS (register) devices and/or computers.

Bursar

Definition: Credit card information is collected by BGSU departments and processed through the Bursar's Office.

Applicable Parties: Determined by low frequency of business manually collected by the departments and processed by the Bursar.

ANNUAL ASSESSMENT:

Each department accepting credit cards will be required to complete an online annual Self Assessment Questionnaire (SAQ). The applicable processing type will determine the SAQ to be completed by each department. Assistance in determining the appropriate SAQ Type will be provided.

SAQ Type	Description
A	**Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced.** ***This would never apply to face-to-face merchants.***
B	**Imprint-only merchants with no electronic cardholder data storage, or standalone, dialout terminal merchants with no electronic cardholder data storage**
C-VT	**Merchants using only web-based virtual terminals, no electronic cardholder data storage**
C	**Merchants with payment application systems connected to the Internet, no electronic cardholder data storage**
D	**All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ.**

DEFINITIONS:

MERCHANT ID - An account number from a merchant bank that allows a company to accept credit-card payments. Merchant banks establish bank accounts for the purpose of enabling companies to accept credit card payments. The merchant bank account allows a company to receive and process credit card transactions online and transfers money from the buyer's account to the seller's account.

PCI DSS COMPLIANCE - The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders

against misuse of their personal information. The PCI DSS was created jointly in 2004 by four major credit-card companies: Visa, MasterCard, Discover and American Express.

SELF ASSESSMENT QUESTIONNAIRE (SAQ) – A validation tool to help merchants validate their compliance with PCI-DSS.

Cardholder data - Full magnetic stripe or the PAN plus any of the following:

- **Cardholder name**
- **Expiration date**
- **Service Code**

BGSU PCI DSS - User Authentication and Access Policy

1.0 Purpose

This policy outlines the authentication and access control requirements when accessing sensitive card data.

2.0 Scope

This policy applies to all users in the (Card Processing Environment) CPE at BGSU.

3.0 Policy

3.1 Identification

Ensure proper user identification and authorization.

3.1.1 User accounts must use a unique identifier, no group or shared accounts are permitted

3.1.2 Verify user identity prior to making any changes including additions, deletions or modifications.

3.1.3 Users must annually acknowledge understanding of the account policy and procedures. Accounts must conform to the following parameters.

3.1.3.1 First time passwords must be unique and changed upon first use
3.1.3.2 Passwords must change every 90 days
3.1.3.3 Do not use group or shared passwords
3.1.3.4 Passwords must be *Strong*
3.1.3.5 Passwords cannot be the same as the last 4 used
3.1.3.6 Accounts must utilize at least a 30 minute lockout when failure attempts exceed 6.
3.1.3.7 Passwords must be rendered unreadable and utilize strong cryptography on any storage system.

3.1.4 System access must be logged. Success and failure access to all system data must be logged and retained for at least 1-year. Logs must be kept online and available for 90 days.

3.1.5 Vendor accounts must only be enabled during the time that they are needed.

3.2 Access

Restrict access to data on a "need to know" basis.

3.2.1 Authorization must be completed on a form signed by management defining access.

3.2.2 An automated access control system must be in place.

3.3 Removal

3.3.1 A process must exist to disable and remove accounts that are no longer needed immediately.

3.3.2 User Accounts must be reviewed, inactive accounts shall be retired at least every 90 days.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the Department, or the University.

PCI Requirements Reference

7.1 ***Limit access to system components and cardholder data to only those individuals whose job requires such access.***

7.1.1 ***Restriction of access rights to privileged user IDs to least privileges necessary to perform job***
Responsibilities

7.1.2 ***Assignment of privileges is based on individual personnel's job classification and function***

7.1.3 ***Requirement for an authorization form signed by management that specifies required privileges***

7.1.4 ***Implementation of an automated access control system***

7.2 ***Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*** This access control system must include the following:

7.2.1 ***Coverage of all system components***

7.2.2 ***Assignment of privileges to individuals based on job classification and function***

7.2.3 ***Default "deny-all" setting***

8.1 ***Assign all users a unique ID before allowing them to access system components or cardholder data*****.**

8.2 ***In addition to assigning a unique ID****,* ***employ at least one of the following methods to authenticate all users:***

a. ***Password or passphrase***

b. ***Two-factor authentication (for example, token devices, smartcards, biometrics, or public keys***

8.3 ***Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.***

8.4 ***Render all passwords unreadable during transmission and storage on all system components using strong cryptography***

8.5 & sub ***Ensure proper user authentication and password management for non-consumer users and administrators on all system components….***

BGSU PCI DSS – IT Policy

INTRODUCTION:

Bowling Green State University provides information technology resources to support the academic, administrative, educational, research and service missions of its appropriately affiliated members within the margins of institutional priorities and financial capabilities. The information technology resources provide for the University, a conduit for free and open forum for the expression of ideas mindful of the University core values. In order to protect the confidentiality, integrity, and availability of information technology resources for intended purposes, the following policy has been developed. The scope of this policy is to encompass all information technology devices owned by the University, any device obtaining connectivity to the University network, and all University relevant data on these devices.

POLICY:

1. **All usage of information technology resources is to be consistent with all other relevant policies at BGSU. [details]**
2. **Users must be aware of and comply with all Federal, State, local, and other applicable laws, contracts, regulations and licenses. [details]**
3. **Use of information technology to access resources other than those supporting the academic, administrative, educational, research and service missions of the University or for more than limited social purposes is prohibited. [details]**
4. **All users must only access or attempt to access information technology resources that they are authorized to use and then only in a manner and to the extent authorized. [details]**
5. **Attempting to circumvent information technology security systems is prohibited. [details]**
6. **Disruption of University authorized activities is prohibited. [details]**
7. **Use of information technology to conduct reconnaissance, vulnerability assessments, or similar activity by unauthorized personnel is prohibited. [details]**
8. **Users are required to protect the confidentiality, integrity, and availability of information technology. [details]**
9. **Anonymous use, impersonation, or use of pseudonyms on an information technology resource to escape accountability is prohibited. [details]**
10. **The use of any unlicensed spectrum space is prohibited on any BGSU-owned or BGSU-occupied property, unless it is part of the wireless services being deployed by the University. [details]**

RESPONSIBILITIES

University Responsibilities

-
    - **Provide and coordinate information technology resources to allow completion of duties as assigned in support of the academic, administrative, educational, research, and service missions, within the margins of institutional priorities and financial capabilities**
    - **Communicate, review, update, and enforce policies to protect information technology resources**
    - **Take reasonable measures to mitigate security threats**

User Responsibilities

-
    - **Read, agree to, and abide by all University policies and policy updates**
    - **Practice safe computing when using information technology resources**
    - **Notify University officials upon discovery that an assigned information technology resource has been accessed, attempted to be accessed, or is vulnerable to access by unauthorized users**
    - **Users are responsible for activity resulting from their assigned information technology resources**

SECURITY AND PRIVACY STATEMENT

BGSU respects the privacy of all information technology users. The University does not routinely monitor the content of material but does reserve the right to access and review all aspects of its information technology infrastructure to investigate performance or system problems, search for harmful programs, or upon reasonable cause, to determine if a user is violating a policy, State or Federal law. BGSU monitors, keeps, and audits detailed records of information technology usage; traces may be recorded routinely for trouble shooting, performance monitoring, security purposes, auditing, recovery from system failure, etc.; or in response to a complaint, in order to protect the University's and others' equipment, software, and data from unauthorized use or tampering. Extraordinary record keeping, traces and special techniques may be used in response to technical problems or complaints, or for violation of law, policy or regulations, but only on approval by University administrators specifically authorized to give such approval. In addition to the privacy of individuals being respected under normal circumstances, the privacy of those involved in a complaint will be respected and the University will limit special record keeping in order to do so, where feasible. Information will be released in accordance with law. Users should be aware that while the University implements various security controls to protect information technology resources, protection of data from unauthorized individuals cannot be guaranteed.

ENFORCEMENT AND SANCTIONS

Individuals or entities in violation of the BGSU Information Technology Policy will be referred to the appropriate disciplinary authority for review. Access privileges may be suspended without prior notice if it is determined that a policy violation is causing a current or imminent threat to the confidentiality, integrity, or availability of information technology resources.

DEFINITION OF TERMS

Information Technology Resources

> ***All aspects associated with management and processing of information. This includes facilities, technologies, and data used for University processing, transfer, storage, and communications. Examples of these resources include, but are not limited to, computers, networking equipment, telecommunications equipment, electronic mail, electronic information sources, network bandwidth, wireless devices, video communications, IP telephony, University assigned accounts, voice mail, passwords, access controls, storage media, documentation, personal digital assistants.***

Safe Computing

> ***Using information technology in a secure manner consistent with its intended purpose. Examples of security measures to be taken include, but are not limited to, the use of strong passwords that are not easily guessable, are changed regularly and are kept private; the application of all relevant security patches in a timely manner; maintenance of up-to-date virus definitions; backup and protection of important/critical data; security of passwords; protection of data and files.***

For more terms and definitions, please visit: http://www.bgsu.edu/offices/cio/page51659.html

BGSU PCI DSS - Physical Security Policy

1.0 Purpose

This policy outlines the physical constraints required to protect data and facilities in the CPE.

2.0 Scope

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers at BGSU including all personnel affiliated with third parties. This policy applies to all data and facilities involved in the CPE at BGSU.

3.0 Policy

3.1 Access

All equipment that is involved in the CPE must be maintained in a secure environment. Only personnel involved in the CPE should be allowed access to the data center.

3.2 The data center must limit access via badging, lock, or some other management approved security. Logs (electronic or paper) of ingress and egress to the center must be maintained.

3.3 Authorized Personnel must be badged or easily distinguished from the public

3.4 Visitors must be badged or given some physical token that distinguishes them from employees. This token must expire at a specific time and be surrendered at the time of departure from the facility.

3.5 Restrict access to physical network jacks, wireless access points, and routers. Unless in use, switch and router ports will be disabled.

3.6 System and audit logs showing access to this data must be retained for at least 1-year. 90 days must be kept online and available for 90 days.

3.7 Physically secure all paper and electronic media that contains cardholder data. "working documents" may be locked in a cabinet during the day, but must be returned to a safe or approved storage facility at the end of the day.

3.8 Fax machines, POS devices and other equipment used for processing cardholder data must be in a secure cabinet or safe when not in use.

3.9 Security

3.9.1 All sensitive and credit card data must be kept secure at all times. The use of man-traps, cameras, electronic controls are authorized to protect the facility.

3.9.2 Review of logs and camera systems shall be completed on a monthly basis.

4.0 Enforcement

4.1 Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the Department, or the University.

PCI Requirements Reference

9.1 *Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.*

9.1.1 *Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law*

9.4 *Use a visitor log to maintain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law.*

9.6 *Physically secure all paper and electronic media (including computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, etc).*

9.9 *Maintain strict control over the storage and accessibility of media that contains cardholder data.*

9.6 *Obtain the policies and procedures for protecting all paper and electronic media that contains cardholder data. Verify that the process includes controls for paper and electronic media in computer rooms and data centers, as well as paper receipts, paper reports, faxes, CDs and disks in employee desks and open workspaces, and PC hard drives.*

9.7 *Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data including the following:*

9.7.1 *Classify the media so it can be identified as confidential.*

9.7.2 *Send the media by secured courier or other delivery methods that that can be accurately tracked*

9.10 ***Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:***
9.10.1 ***Cross-cut shred, incinerate, or pulp hardcopy materials.***
9.10.2 ***Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.***

BGSU PCI DSS Card Processing Environment Hardware Security Policy

1.0 Purpose

To establish a baseline security configuration policy for all payment Card Processing Environments (CPE) owned, operated, or managed by *BGSU.* All CPEs will remain compliant with the PCI DSS*.

2.0 Scope

This policy applies to all networks and systems used in the *BGSU* CPEs

3.0 Policy

3.1 Documentation

3.1.1 Configurations of the network and systems involved in the CPE will be standardized and documented. Details shall include: Names, addressing, data flow and separation from non-CPE traffic. Standards shall address all known security vulnerabilities and are consistent with accepted industry hardening standards.

3.1.2 Roles and responsibilities for logical management of network components shall be identified and documented. Roles include but not limited to: Security Admin, Network Admin, Approval admin, etc.

3.1.3 All services, protocols and ports allowed 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.

3.2 General Configuration rules

3.2.1 If SNMP is to be used, community strings will be changed from default values.

3.2.2 System clocks on all equipment must be synchronized to a centralized time source.

3.2.3 All remote console access shall be encrypted using standard strong encryption techniques.

3.2.4 Configuration changes must be submitted to an authority for approval. Any changes must; be documented and dated, tested, and include rollback procedure.

3.2.5 Document all process and procedures defining discovery of new security vulnerabilities and update defined configuration standards accordingly.

3.3 Firewalls

CPE networks will have a hardware based stateful packet inspection firewall installed at all Internet connections and between any non-CPE internal network, or DMZ. Firewalls will be configured:

3.3.1 To deny all incoming traffic and will have exceptions based upon the specific business requirements of the CPE.

3.3.2 To deny all outgoing traffic and will have exceptions based upon the specific business requirements of the CPE.

3.3.3 To have default vendor passwords changed prior to being installed on the network.

3.3.4 To disallow any direct traffic between the CPE and Internet.

3.3.5 To allow management access from authorized workstations only specified by IP address

3.3.6 Logging will be enabled and will log all incoming and outgoing connections. Logs will be maintained in a separate location on a separate logging device. Logs must be available for at least one year.

3.3.7 All CPE Firewall rule sets will be reviewed at least bi-annually.

3.3.8 Reviews must be documented and dated

3.3.9 Running and startup configurations must be synchronized.

3.4 Network Equipment

3.4.1 All networking equipment (switches, routers, IDS/IPS, etc.) will have default vendor passwords changed prior to being installed on the network

3.4.2 All connections to the CPE will be fully documented

3.4.3 At no time will there be an active port that is not connected to a CPE device

3.4.4 All requests for changes to the CPE must be documented and approved.

3.4.5 All devices will have logging enabled. Logs will be maintained in a separate location on a separate logging device. Logs must be available for at least 1 year.

3.5 CPE Servers and Workstations

3.5.1 Servers and Workstations connected to the CPE will be installed and configured according to security best practices

3.5.2 Software installations will be limited to approved software necessary for the operations of the CPE

3.5.3 Unnecessary protocols and services will be uninstalled, or made non-functional.

3.5.4 A host based firewall will be in operation and will deny all incoming traffic by default and will have exceptions for critical business functions only

3.5.5 File integrity monitoring software must be in place and setup properly on all critical systems within the CPE.

3.5.6 *Local Administrator* and *Guest* accounts will be disabled

3.5.7 Idle sessions shall require re-input of password to re-enable session.

3.5.8 Access to the system BIOS will be protected via a password mechanism where available

3.5.9 Antivirus software will be installed, running, current and capable of providing audit logs at all times on all CPE machines that are currently susceptible to such compromises.

3.5.10 Servers participating in the CPE will have their security logs forwarded to a server external to the CPE

3.5.11 Operating system patches will be installed within 1 month of release

3.6 Vulnerability Assessments

3.6.1 Vulnerability scans will be completed quarterly on all systems in the CPE. Urgent, critical or high vulnerabilities will be addressed immediately and systems re-scanned for complete remediation.

3.6.2 External and internal penetration tests shall be completed annually and after any significant change to the infrastructure.

3.7 Change Request Procedure

3.7.1 A written request for a configuration change must come from an authorized individual. The request will include a description, the business reason, a start and end date, and a rollback procedure.

3.7.2 The IT Administrator will review the change and determine the scope of work involved.

3.7.3 The Manager will review the change and approve or deny the change in whole or in part.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by the (*Department or University)*.

PCI Requirements Reference

1.1 ***Establish firewall and router configuration standards that include the following:***

1.1.1 ***A formal process for approving and testing all network connections and changes to the firewall and router configurations***

1.1.2 ***Current network diagram with all connections to cardholder data, including any wireless networks***

1.1.3 ***Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone***

1.1.4 ***Description of groups, roles, and responsibilities for logical management of network components***

1.1.5 ***Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure***

1.1.6 ***Requirement to review firewall and router rule sets at least every six months***

1.2 ***Build a firewall configuration that restricts connections between un-trusted networks and any system components in the cardholder data environment.***

1.2.1 ***Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.***

1.2.2 ***Secure and synchronize router configuration files.***

1.2.3 ***Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.***

1.3 ***Prohibit direct public access between the Internet and any system component in the cardholder data environment.***

1.3.1 ***Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.***

1.3.2 ***Limit inbound Internet traffic to IP addresses within the DMZ.***

1.3.3 ***Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.***

1.3.4 ***Do not allow internal addresses to pass from the Internet into the DMZ.***

1.3.5 ***Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.***

1.3.6 ***Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)***

1.3.7 ***Place the database in an internal network zone, segregated from the DMZ.***

1.3.8 ***Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).***

1.4 ***Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.***

2.1 ***Always change vendor-supplied defaults*** *before* ***installing a system on the network—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.***

2.1.1 For wireless environments ***connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.***

2.2 ***Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.***

2.2.2 ***Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).***

2.2.3 ***Configure system security parameters to prevent misuse.***

2.2.4 ***Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.***

2.3 ***Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for Web-based management and other non-console administrative access.***

5.1 ***Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).***

5.1.1 ***Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.***

5.2 ***Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.***

6.1 ***Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.***

6.4 ***Follow change control procedures for all changes to system components. The procedures must include the following:***

6.4.1 ***Documentation of impact***
6.4.2 ***Management sign-off by appropriate parties***
6.4.3 ***Testing of operational functionality***
6.4.4 ***Back-out procedures***

8.5.15 ***If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.***

10.4 ***Synchronize all critical system clocks and times.***

11.2 ***Run internal and external network vulnerability scans at least quarterly and after any significant change in the network .***

11.3 ***Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification. (such as an operating system upgrade, a sub-network added to the environment, or a Web server added to the environment) Penetration tests must include the following:***

11.3.1 ***Network-layer penetration tests***
11.3.2 ***Application layer penetration tests***

BGSU PCI DSS - Software Development Policy

2.0 Purpose

This policy outlines the security and requirements for any development of payment application software or Web based applications that transmit, process or store credit card information.

3.0 Scope

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers at BGSU, including all personnel affiliated with third parties. This policy applies to all networks and data in the CPE at BGSU.

4.0 Policy

4.1 Development Environment

Any software development must be done on a separate development / test infrastructure. It is strictly prohibited to develop or change production software on production systems without following the approved "*Change Control Policy".*

4.1.1 Production data may not be used in any development without being sanitized and all identifying sensitive data removed.

4.1.2 Test data, (IDs, accounts, data, etc) must be removed prior to system being put into production.

4.1.3 Development staff and production staff must maintain a strict separation of duties.

4.1.4 Display of credit card information within an application should be masked in accordance with the PCI DSS. Only the first 6 digits and the last 4 may be displayed.

4.1.5 A separate code review by an impartial group or automated software will be completed prior to software being placed in the production environment.

4.1.6 Strict adherence to industry "best practices" and secure coding practices need to be adhered to in all aspects of the development of applications. For a definition of best practices, refer to http://owasp.org, http://csrc.nist.gov/

4.2 Development Lifecycle

4.2.1 All Web based applications will be scanned for vulnerabilities by a 3rd party on an annual basis or when significant changes have been made.

4.2.2 When applications are no longer needed, they must be securely removed and all data destroyed or rendered unreadable. Backups of the system and development software should also be securely deleted / removed.

4.2.3 System change control procedures must be implemented and logged.

4.2.4 A rollback procedure must be documented and approved prior to any system change.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the Department, or the University.

PCI Requirements Reference

6.3 *Develop software applications based on industry best practices and include information security throughout the software development life cycle.*

6.3.1 *Testing of all security patches and system and software configuration changes before deployment.*

6.3.2 *Separate development/test and production environments.*

6.3.3 *Separation of duties between development/test and production environments.*

6.3.4 *Production data (real credit card numbers) are not used for testing or development.*

6.3.5 *Removal of test data and accounts before production systems become active.*

6.3.6 *Removal of custom application accounts, usernames, and passwords before applications become active or are released to customers.*

6.3.7 *Review of custom code prior to release to production or customers, to identify any potential coding vulnerability.*

6.5 & sub *Develop all web applications based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. See www.owasp.org - "The Ten Most Critical Web Application Security Vulnerabilities." Cover prevention of common coding vulnerabilities in software development processes, to include the following:*

6.6 *Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:*

- *Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security*
- *Installing an application layer firewall in front of web-facing applications.*

BGSU PCI DSS - Data Retention and Disposal

1.0 Purpose

This policy outlines the storage and disposal procedure for all confidential or sensitive data, when no longer needed for card processing requirements. Data must be removed from *BGSU* systems using an approved method documented in this policy. This requirement includes all CPE data stored in systems, temporary files or contained on storage media.

2.0 Scope

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers at BGSU, including all personnel affiliated with third parties. This policy applies to all CPE data in the BGSU network.

3.0 Policy

3.1 Storage

3.1.1 The following credit card information is permitted to be stored as long as there is a business need. Written justification must be provided documenting the business need for retention. (refer to chart in PCI DSS "Applicability Information".) All data must be protected as described in all sections of the PCI DSS.

3.1.1.1 Primary Account Number (PAN)
3.1.1.2 Cardholder name
3.1.1.3 Service Code
3.1.1.4 Expiration Date

3.1.2 Data that is not permitted to be stored includes the following: (exception to this is in "pre-authorization" see 4.3

3.1.2.1 Full Magnetic Stripe (Track 1 or 2 data)
3.1.2.2 CVV2, CVC2, CID, CAV2
3.1.2.3 PIN / PIN Block

3.1.3 Pre-authorization Data including track, CVV2, and PIN information, will be retained only until completion of the authorization of a transaction. Storage of cardholder authorization data post-authorization is forbidden.

3.1.4 System and audit logs showing access to this data must be retained for at least 1-year. Logs must be kept online and available for 90 days.

3.2 Disposal

All sensitive and credit card data must be destroyed when it is no longer required by legal, contractual, or business need. Currently *Business Operations* dictates this timeframe to be *(xx days/months/years.)*

3.2.1 Techniques for disposal data on media is as follows:

  - Hard disks**: must be overwritten by an NSA approved method, smashed, pulverized or otherwise destroyed.**
  - Floppy disks**: must be shredded.**
- Optical media **(CD's, DVD's, Blue Ray, etc.) must be shredded**
- Other magnetic media**, (USB Drives, storage cards, etc) must be overwritten by an approved method, or otherwise destroyed.**
- Paper**: must be cross-cut shredded or incinerated**

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the Department, or the University.

PCI Requirements Reference

*3.1 **Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.***

*3.2 **Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:***

*9.10 **Destroy media containing cardholder data when it is no longer needed for business or legal reasons as
follows:***

*9.10.1 **Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.***
*9.10.2 **Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.***

BGSU PCI DSS - Logging Controls Policy

1.0 Purpose

This policy outlines the process for logging all actions that occur in the CPE. Type and scale of logging, appropriate storage, encryption and disposal of logs is to be adhered to remain compliant with the PCI DSS.

2.0 Scope

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers at BGSU including all personnel affiliated with third parties. This policy applies to all CPE data and systems in the BGSU network.

3.0 Policy

Logging is to be done to the level of detail to assist in the reconstruction of any event that takes place in the CPE. Therefore a secure environment for log acquisition and storage is to be in place.

3.1 Events to be logged

3.1.1 The following events shall be logged

3.1.1.1 User access to any cardholder data

3.1.1.2 Date & Time

3.1.1.3 Type of event

3.1.1.4 Origination

3.1.1.5 Identity of affected data, system or resource.

3.1.1.6 Administrative access to any system that contains cardholder data and specific access of data.

3.1.1.7 All authentication attempts, (pass or fail)

3.1.1.8 Creation or deletion of system level objects

3.1.1.9 Configuration changes

3.1.1.10 Access and changes to root or kernel system files

3.1.1.11 Access and changes to log files

3.2 Storage

All logs must be stored Logs should not be stored on the same system that they events take place, (authentication of users on a domain controller for example). Logs should be written off to a separate robust system that has its own specific security parameters on the internal LAN.

3.2.1 Limit access to logs to authorized personnel.

3.2.2 Logs shall be dated on a daily basis

3.2.3 A file integrity monitoring software shall be installed to monitor all access and changes to log files.

3.2.4 Logs shall be retained for at least 1 year.

3.2.5 Audits must be conducted to verify the viability of logs

3.2.6 Logs must be reviewed daily. It is permitted to incorporate software for this purpose. The appropriate triggers and alerts must be setup and tested regularly.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the Department, or the University.

PCI Requirements Reference

10.1 *Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user*

10.2.1 *All individual user accesses to cardholder data*

10.2.2 *All actions taken by any individual with root or administrative privileges*

10.2.3 *Access to all audit trails*

10.2.4 *Invalid logical access attempts*

10.2 5 *Use of identification and authentication mechanisms*

10.2.6 *Initialization of the audit logs*

10.2.7 *Creation and deletion of system-level objects.*

10.3 & sub *Record at least the following audit trail entries for all system components for each event:*

10.5 & sub *Secure audit trails so they cannot be altered.*

10.6 *Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).*

BGSU PCI DSS - Backup Control Policy

1.0 Purpose

This policy outlines the control of all backup subsystems and the data therein involved in the CPE. Storage, identification, transport, isolation, encryption and disposal of media utilized in the backup systems.

2.0 Scope

This policy applies to all systems, data and affiliated third parties encompassing the CPE in the BGSU network.

3.0 Policy

3.1 Storage

The backup subsystem must be identified as part of the CPE. Cardholder data on the subsystem must be rendered unreadable and unable to be re-constructed through un-approved means. Backups of sensitive data must be completed on a regular basis. Data should be checked regularly for restoration applicability.

3.1.1 Pre-authorization Data including track, CVV2, and PIN information, will be retained only until completion of the authorization of a transaction. Storage of cardholder authorization data post-authorization is forbidden.

3.1.2 System and audit logs showing access to this data must be retained for at least 1-year. 90 days must be kept online and available for 90 days.

3.2 Control

3.2.1 All media with sensitive data must be marked as confidential and strict control must be maintained in storage and accessibility of the media.

3.2.2 Media must be stored in a secure location approved by management. This location must have limited accessibility to only those that need access. All access to the location must be logged. Security of facility must be reviewed annually.

3.2.3 All media couriers and transport mechanisms must be certified by Business Operations,

3.2.4 Any media sent outside the control of the Information Technology facility must be positively logged in and out. A record must be maintained of all media in storage and use as well as its whereabouts.

3.3 Disposal

All media that is no longer needed or has reached end-of-life must be destroyed or rendered unreadable so that no data may be extracted. Information on acceptable destruction techniques is detailed in the *Data Retention and Disposal policy*.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the Department, or the University.

PCI Requirements Reference

9.5 *Store media back-ups in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.*

9.7.1 *All media should be classified so that it can be identified as "confidential".*

9.7.2 *All media sent outside the facility is logged and authorized by management, and sent via secured courier or other delivery mechanism that can be tracked.*

9.8 *Ensure management approves all media that is moved from a secured area (especially when media is distributed to individuals).*

9.9 ***Maintain strict control over the storage and accessibility of media that contains cardholder data.***

9.10.2 ***Render cardholder data on electronic media unrecoverable so that cardholder data cannot be***
re-constructed.

BGSU PCI DSS - Shared Data – Service Provider Policy

1.0 Purpose

This policy outlines the operating and contractual procedure for sharing all confidential or sensitive data with a 3rd party.

2.0 Scope

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers at BGSU including all personnel affiliated with third parties. This policy applies to all CPE data in the BGSU network.

3.0 Policy

Third parties, with whom cardholder data is shared, are contractually required to adhere to the PCI DSS requirements and to acknowledge that they are responsible for the security of the cardholder data which they process. Only the minimum amount of data needed to complete the transaction will be shared with a 3rd party. All interaction must be documented and logged.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the Department, or the University.

PCI Requirements Reference

*2.4 **Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.***

BGSU PCI DSS - Wireless Usage Policy

1.0 Purpose

This policy outlines the requirements for using wireless communications to transmit sensitive credit card information. These requirements are outlined in the PCI DSS section 4

2.0 Scope

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers at BGSU including all personnel affiliated with third parties. This policy applies to all CPE data in the BGSU network. This applies to all wireless technologies used to transmit data to include but not limited to: IEEE 802.11 wireless, GSM and GPRS.

3.0 Policy

3.1 Usage

Communications must utilize industry standard best practices to implement strong encryption for authentication and transmission

3.1.1 WPA2 is the standard encryption

3.1.2 WEP shall not be permitted in use after June 30, 2010

3.2 Encryption

Strong encryption keys must be used for wireless communication. Encryption must follow the same process as those described in the encryption policy.

3.3 Wireless Accounting

Scanning must be completed quarterly to verify that no un-authorized wireless networks have been installed in the CPE. If scanning is not feasible, a Wireless Intrusion Detection / Protection system may be used.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the Department, or the University.

PCI Requirements Reference

4.1.1 *For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi Protected Access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS at 128-bit. Never rely exclusively on WEP to protect confidentiality and access to a wireless LAN. Use one of the above methodologies in conjunction with WEP at a minimum 104-bit encryption key and 24 bit-initialization value, (recommend 128 bit key) and rotate shared WEP keys quarterly (or automatically if the technology permits) and whenever there are personnel changes. Restrict access based on MAC address.*

2.1.1 *For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.*

11.1 ***Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.***

BGSU PCI DSS - Encryption

1.0 Purpose

All confidential or sensitive electronic data within the *BGSU* CPE must be protected by approved encryption techniques. This policy applies to the management of encryption keys and application of their use.

2.0 Scope

This policy applies to all faculty, staff, students, contractors, consultants, temporary, and other workers at BGSU including all personnel affiliated with third parties. This policy applies to all CPE data in the BGSU network.

3.0 Policy

3.1 Encryption Keys

3.1.1 Only Strong encryption can be utilized to protect sensitive data. These methods are defined by the PCI DSS;

3.1.1.1 3DES

3.1.1.2 AES

3.1.1.3 Proprietary Vendor encryption providing it is approved in the PA-DSS

3.1.1.4 SSL

3.1.1.5 IPSEC

3.1.2 Encryption keys must protected in the following manner;

3.1.2.1 Have dual custodianship with the fewest number of custodians.

3.1.2.2 Clear text images of the keys must be kept locked in a tamper proof manner and in the fewest possible locations and forms.

3.1.3 System and audit logs showing access to this data must be retained for at least 1-year. 90 days must be kept online and available for 90 days.

3.2 Documentation

3.2.1 All process and procedures for the generation, use and destruction of cryptographic keys must be fully documented.

3.2.2 Require key custodians to acknowledge and accept responsibilities of their role as such by use of a formal signature.

3.3 Use

3.3.1 All protected data whether at rest or online, must be rendered unreadable. Techniques such as encryption, truncation, 1-way hashing, tokenization, etc.

3.3.2 If disk encryption is used as opposed table or file encryption, tables in databases holding sensitive information must be protected using techniques listed above.

3.3.3 All data exchanged between systems and third parties must be done utilizing these strong encryption techniques.

3.3.4 Keys must be rotated at a minimum of 1 year intervals

3.4 Destruction

3.4.1 Old keys must be destroyed when no longer used, or confidence in the keys integrity may have become compromised.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the Department, or the University.

PCI Requirements Reference

3.4.1 ***If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.***

3.5 *Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:*

3.5.1 *Restrict access to keys to the fewest number of custodians necessary.*

3.5.2 *Review system configuration files to determine that storage of cryptographic keys in encrypted format and storage of key-encrypting keys separately from data-encrypting keys.*

3.6.1 *Generation of strong cryptographic keys.*

3.6.2 *Secure cryptographic key distribution.*

3.6.3 *Secure cryptographic key storage.*

3.6.4 *Periodic cryptographic key changes.*

- *As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically*
- *At least annually.*

3.6.5 *Retirement or replacement of old or suspected compromised cryptographic keys..*

3.6.6 *Split knowledge and establishment of dual control of cryptographic keys*

3.6.7 *Prevention of unauthorized substitution of cryptographic keys.*

3.6.8 *Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key custodian responsibilities*

4.1 *Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public network.*