Grand Valley State University

Information Security Policies and Procedures

January 2024

Revision History

Changes	Approving Manager	Date
Initial Publication	Susan K. Korzinek	4/18/2010
Revised based on 3.2 specifications	Susan K. Korzinek	1/04/2017
Reviewed	Susan K. Korzinek	2/26/2018
Revised based on 3.2.1 specifications	Susan K. Korzinek	8/7/2018
Review process	Susan K. Korzinek	8/28/19
Review process	Susan K. Korzinek	9/24/20
Review Process	Susan K. Korzinek	1/12/2021
Review Process	Luke DeMott	8/2/2024

Table of Contents

1 INTRODUCTION AND SCOPE

1.1 Introduction

This document explains Grand Valley State University (GVSU)'s information security requirements for all employees. GVSU's management has committed to these security policies to protect information utilized by GVSU in attaining its business goals. All employees whose responsibilities include cardholder data processing are required to adhere to the policies described within this document.

1.2 What is Payment Card Industry (PCI) Compliance?

The Payment Card Industry Data Security Standard (PCI DSS) Program is a mandated set of security standards that were created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding cardholder data for all credit card brands.

In September of 2006, a group of five leading payment brands including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International jointly announced formation of the PCI Security Standards Council, an independent council established to manage ongoing evolution of the PCI standard.

PCI DSS requirements apply to any entity that stores, processes or transmits cardholder data. The requirements apply to all methods of credit card processing, from manual to computerized; the most comprehensive and demanding of which apply to e-commerce websites, and retail POS systems that process credit cards over the Internet. This document addresses all the requirements of the Payment Card Industry Data Security Standard (PCI DSS). For more information about this standard, visit the official website at: https://www.pcisecuritystandards.org.

1.3 Scope of Compliance

The PCI requirements apply to all "system components." System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is defined as part of the network that possesses cardholder data or sensitive authentication data. For example, the following types of systems would be in scope for compliance within any environment:

- Systems storing cardholder data (e.g. databases, PC's used by accounting for generating reports)
- Systems processing cardholder data (e.g. web servers, application servers, etc.)
- Network devices transporting or directing cardholder traffic (e.g. border router, DMZ firewall, intranet firewall, etc.)
- Devices that create media containing cardholder data (e.g. fax machine, printer, backup tape silo)
- Support systems (e.g. Active Directory, syslog server, IDS, PC's performing support functions such as system administration, etc.)
- Custom software developed by or for Grand Valley State University
- Datacenter operations (e.g., video cameras, badges, visitor logs, etc.)

- Systems that provide security services (for example, authentication servers), facilitate segmentation (for example, internal firewalls), or may impact the security of (for example, name resolution or web redirection servers) the CDE.
- Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.
- Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
- Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).
- Applications including all purchased and custom applications, including internal and external (for example, Internet) applications.
- Any other component or device located within or connected to the CDE.

These policies and procedures shall only apply within the PCI environment identified in the *PCI Environment Description (Appendix P)*.

2 POLICY ROLES AND RESPONSIBILITIES

2.1 Policy Applicability

All employees, contractors, vendors and third parties that use, maintain or handle GVSU information assets must follow this policy. Policy exemptions will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

PCI Requirements Reference:

Testing Procedure 12.4.a. Verify that information security policies clearly define information security responsibilities for all personnel.

Testing Procedure 12.4.b. Interview a sample of responsible personnel to verify they understand the security policies.

2.2 Chief Information Security Officer

The Chief Information Security Officer is responsible for coordinating and overseeing GVSU wide compliance with policies and procedures regarding the confidentiality, integrity and security of its information assets.

The Chief Information Security Officer works closely with other GVSU managers and staff involved in securing the company's information assets to enforce established policies, identify areas of concern, and implement appropriate changes as needed. Specific responsibilities of the Chief Information Security Officer include:

- Make high-level decisions pertaining to the information security policies and their content. Approve, in advance, exceptions to these policies on a case-by-case basis.
- On an annual basis, or upon significant changes to the environment, coordinate a formal risk assessment to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks.
- Annually review the Information Security policies and procedures to maintain adequacy in light of emergent business requirements or security threats.
- Make sure that all third parties, with whom cardholder data is shared, are handled according to the *Third Parties and Third Party Agreements Policy (Section 17)*.
- Maintain, update and distribute the Incident *Response Plan and Procedures (Section 14)* to all users.
- Information Technology Department is responsible to verify that employees are provided security awareness training upon hire and at least annually.
- Information Technology Department is responsible for disseminating security awareness information to system users utilizing multiple methods of communicating awareness and educating employees (e.g. newsletters, memos, web based training, meetings, etc.).
- Chief Information Security Officer will maintain all *Security Awareness and Acceptable Use (Appendix A)* forms on employees via the eDocument system and/or third party cybersecurity training.
- *Authorization Request Forms (Appendix G)* are requested and managed via email by each individual department. Approval must be via an authorized supervisor of the department.

- On an annual basis, consult with the different business units to confirm that any new acceptance channels for credit cards have been included in the scoping process. Any changes in the scope must be updated in the *PCI Environment Description (Appendix P)*.
- Complete tasks as required by the *Periodic Operational Security Procedures (Appendix N)*.
- Maintaining an up-to-date cardholder data flow diagram. The diagram must include the date when it was last updated.

PCI Requirements Reference:

Testing Procedure 12.1. Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).

Testing Procedure 12.1.1. Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

Testing Procedure 12.5. Examine information security policies and procedures to verify:

- The formal assignment of information security to a Chief Information Security Officer or other security-knowledgeable member of management
- The following information security responsibilities are specifically and formally assigned:

Testing Procedure 12.5.3. Verify that responsibility for creating and distributing security incident response and escalation procedures is formally assigned.

2.3 Information Technology Department

Successfully securing GVSU information systems requires that the various departments and groups consistently adhere to a shared vision for security.

The Information Technology Department works with departmental system managers, administrators and users to develop security policies, standards and procedures to help protect the assets of GVSU.

The Information Technology Department is dedicated to security planning, education and awareness. Specific responsibilities of the Information Technology Department include:

- Create new information security policies and procedures when needs arise. Maintain and update existing information security policies and procedures. Review the policy on an annual basis and assist management with the approval process.
- Act as a central coordinating department for implementation of the Information Security Policies.
- Create, maintain and distribute incident response and escalation procedures.
- Control and monitor access to restricted areas and confidential data. Ensure appropriate physical controls are in place where cardholder information is present.
- Complete tasks as required by the *Periodic Operational Security Procedures (Appendix N)*.

PCI Requirements Reference:

10.6 Review logs and security events for all system components to identify anomalies or suspicious activity.

Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.

Testing Procedure 10.6.1.a. Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools:

- All security events
- Logs of all system components that store, process or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD, logs of all
- Logs of all critical system components
- Logs of all servers and system components that perform security functions.

Testing Procedure 10.6.1.b. Observe processes and interview personnel to verify the following are reviewed at least daily:

- All security events
- Logs of all system components that store, process or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD, logs of all
- Logs of all critical system components
- Logs of all servers and system components that perform security functions.

Testing Procedure 12.2.a Verify that an annual risk-assessment process is documented that identifies assets, threats, vulnerabilities, and results in a formal risk assessment.

Testing Procedure 12.2.b Review risk assessment documentation to verify that the risk assessment process is verified at least annually and upon significant changes to the environment.

Testing Procedure 12.5.2. Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.

Testing Procedure 12.5.5. Verify that responsibility for monitoring and controlling all access to data is formally assigned.

2.4 System Administrators

GVSU System Administrators are the direct link between information security policies and the network, systems and data. System Administrator responsibilities include:

- Applying GVSU information security policies and procedures as applicable to all information assets.
- Completing tasks as required by the *Periodic Operational Security Procedures (Appendix N)*.

PCI Requirements Reference:

Testing Procedure 1.1.2.a. Verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks.

Testing Procedure 1.1.2.b. Interview responsible personnel to verify that the diagram is kept current.

Testing Procedure 1.1.3. Examine the data-flow diagram and interview personnel to verify the diagram:

- Shows all cardholder data flows across systems and networks
- Is kept current and updated as needed upon changes to the environment.

Testing Procedure 12.5.4. Verify that responsibility for administering user account and authentication management is formally assigned.

2.4.1 Windows Server Administrator

- Administering user account and authentication management for Administrators, based on procedures in section 4.6.

- Support File Integrity Logging on all Windows Servers and Clients, based on criteria in section 8.2.5.
- Support Anti-Virus on all Windows Servers and Clients.

2.4.2 Network Administrator

- Maintaining an up-to-date network diagram. The diagram must include the date when it was last updated. GVSU does not currently support wireless networks or devices on the PCI environment.
- Restricting physical access to publicly accessible network jacks, wireless access points, gateways and hand held devices.

  Maintain an up to date hardware and Software Inventory.
- Quarterly Wireless Rogue Access Point Scans must be performed and any Rogue Access Points that appear to be emulating GVSU Services or pose a security threat must be identified, removed and reported to Information Security. We realize that in a Campus Environment, it's virtually impossible to track down all Rogue Apps.

2.4.3 Information Security Administrator

- Assisting the Information Technology Department with monitoring and controlling all access to GVSU data.
- Review logs daily on Business Days. Follow up on any exceptions identified.
- Setup real time 7x24 email alerts to key staff for Security Incidents.
- Monitor and analyze security alerts and distribute information to appropriate information security, technical and business unit management personnel.
- Take on primary responsibility for Section 8.3 Duties; including assessing vulnerabilities and verifying that Patches and Updates have been applied.
- Review Monthly Nessus Scans and make sure all High and Critical Vulnerabilities are addressed within 2 Weeks.
- Make sure Logs are retained and secured in compliance with Section 5.2.
- Monitor and adjust compliance with section 16 regarding Security and Event Logging.

2.4.4 Application Group Administrator

- Administering user account and authentication management for End Users based on procedures in section 4.6.
- Work with the Network Administrator to maintain an accurate and up to date Hardware and Software Inventory.
- Perform Monthly physical reviews of all Client Machines and Devices.
  - Report Inventory Changes and Discrepancies to the Network Administrator.
  - Verify there aren't any unauthorized USB Devices or Wireless interfaces connected and report anything that's found to the Information Security.
- Review Accounts for your Group Monthly and follow-up on any accounts inactive more than 60 days and delete any accounts inactive more than 90 days.

- Must make sure that all third party Credit Card Processing systems use individual accounts with complex passwords and meet the requirements of section 12.3.
- Must make sure that all client devices are labeled in compliance with section 12.5.

2.5 HR Department

Due to their direct and constant relationship with existing employees, as well as their unique position of having the first and last interactions with new/terminated employees, the HR Department has an important role with regards to GVSU information security. The following items are the ongoing responsibility of the HR Department:

- Assist the Information Technology Department with publishing and disseminating GVSU information security policies and acceptable use guidance to all relevant system users, including vendors, contractors and business partners.
- Perform background checks on new employees who will have access to cardholder data or the PCI environment. When possible and within the constraints of local laws, background checks should include: previous employment history (department responsibility), criminal record, credit history (when requested for positions requiring financial background check), and reference checks (department responsibility). For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, background checks are a recommendation only.
- Work with the Information Technology Department to administer sanctions and disciplinary action relative to violations of the Information Security Policy.
- Notify the IT Department when any employee is terminated. Removal of PCI access to systems is the responsibility of the department the employee works in.

PCI Requirements Reference:

Testing Procedure 12.5.1. Verify that responsibility for creating and distributing security policies and procedures is formally assigned.

Testing Procedure 12.6.a. Review the security awareness program to verify it provides awareness to all personnel about the importance of cardholder data security.

Testing Procedure 12.6.b. Examine security awareness program procedures and documentation and perform the following:

Testing Procedure 12.6.1.a. Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions).

Note: *Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*

Testing Procedure 12.6.1.b. Verify that personnel attend security awareness training upon hire and at least annually.

Testing Procedure 12.6.1.c. Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security.

Testing Procedure 12.7. Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) on potential personnel prior to hire who will have access to cardholder data or the cardholder data environment.

Note: *For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*

2.6 Users

Each user of GVSU computing and information resources must realize the fundamental importance of information resources and recognize their responsibility for the safekeeping of those resources. Users must guard against abuses that disrupt or threaten the viability of all systems. The following are specific responsibilities of all GVSU information system users:

- Understand what the consequences of their actions are with regard to computing security practices and act accordingly. Embrace the "Security is everyone's responsibility" philosophy to assist GVSU in meeting its business goals.
- Maintain awareness of the contents of the information security policies.
- Upon hire and at least annually, read the corporate security policy and sign the *GVSU Security Awareness and Acceptable Use Policies (Appendix A)*.
- Classify confidential and sensitive information that is received unclassified, according to the Data Classification Policy (Section 4.2). Limit the distribution of this information accordingly.

PCI Requirements Reference:

Testing Procedure 12.6.2. Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.

3 IT CHANGE CONTROL POLICY

3.1 Policy Applicability

All proposed changes to GVSU network devices, systems and application configurations must follow this policy. All proposed changes to in-scope components which could affect the security of cardholder data or the cardholder data environment must follow this policy. At a minimum, this must include changes to network connections, firewall and router configuration, system and application configuration changes, security patches, and other changes as required to ensure the environment's security posture is not adversely affected.

3.2 Change Request Submittal

The responsible party that will be implementing the change must follow the *Change Request procedure listed in (Appendix C).*

This form will not be reviewed without the following information:

- **Impact Description** – The impact of the change must be documented so that all the affected parties (internal or external) will be able to plan accordingly for any processing change. In particular, all the systems, users and resources affected by the change must be documented and the criticality of the change must be rated as either high, medium or low.
- **Back out Procedures** – If the change does not go as intended a plan must be in place that describes the process of reverting the environment to its original configuration.
- **Test Plan** - A set of planned tests must be developed to verify that the change accomplished what it was supposed to do, and does not adversely affect other system components or create a weakness in the security posture of the environment. For custom code changes, all updates must be tested for compliance with the *Software Development Policy (Section 13).*
- **Management Approval** – All changes must include management approval.

PCI Requirements Reference:

Testing Procedure 1.1.1.a. Examine documented procedures to verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.

Testing Procedure 1.1.1.b. For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.

Testing Procedure 1.1.1.c. Identify a sample of actual changes made to firewall and router configurations compare to the change records, and interview responsible personnel to verify the changes were approved and tested.

Testing Procedure 6.4.5.a. Verify that change-control procedures related to implementing security patches and software modifications are documented and require items 6.4.5.1 – 6.4.5.4 below.

Testing Procedure 6.4.5.b. For a sample of system components and recent changes/security patches, trace those changes back to related change control documentation. For each change examined, perform the following:

Testing Procedure 6.4.5.1. Verify that documentation of impact is included in the change control documentation for each sampled change.

Testing Procedure 6.4.5.2. Verify that documented approval by authorized parties is present for each sampled change.

Testing Procedure 6.4.5.3.a. For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.

Testing Procedure 6.4.5.3.b. For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.

Testing Procedure 6.4.5.4. Verify that back-out procedures are prepared for each sampled change.

3.3 Change Request Approval

After all planning and documentation is completed, all relevant management must sign-off on the *Change Request Form (Appendix C).*

Approved management personnel are Associate Director of Technical Services or Chief Information Security Officer.

3.4 Change Testing

Due to the limit size and scope of our PCI Environment, it may not be practical to pre-test all changes, and we have the option of a post-deployment test with a good rollback plan.

Testing of all security patches, system and software configuration changes must be performed.

The documented test plan must be followed to ensure no adverse effects on the network, systems or applications. Any discrepancies should be documented and a new *Change Request Form (Appendix C)* generated once all issues have been resolved.

3.5 Change Implementation

All changes must be implemented according to the documented change procedures that were tested successfully. Any discrepancies between expected results and actual results that impact the network, systems, applications, business requirements or support procedures must result in the immediate invocation of the documented back out procedures.

4 DATA CLASSIFICATION AND CONTROL POLICY

4.1 Policy Applicability

All data stored and accessed on GVSU information systems, whether managed by employees or by a third party, must follow this policy. Policy exemptions will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

Note: No cardholder data is stored on GVSU computing resources, media or paper.

4.2 Data Classification

4.2.1 Introduction

All data stored on GVSU computing resources must be assigned a classification level by the information owner or creator. This level is used to determine which users are permitted to access the data.

4.2.2 Information Categories

- **Confidential** - Applies to the most sensitive business information which is intended strictly for use within GVSU. Unauthorized disclosure could seriously and adversely impact the company, stockholders, business partners, and/or its customers. Examples of confidential information include passwords, encryption keys, cardholder data, bank account information, etc.
- **Sensitive** - Applies to less sensitive business information which is intended for use within GVSU. Unauthorized disclosure could adversely impact the company, its stockholders, its business partners, and/or its customers. Examples of sensitive information include, internal market research, audit reports, etc.
- **Private** - Applies to personal information which is intended for use within GVSU. Unauthorized disclosure could adversely impact the company and/or its employees. Examples of private information include policies and procedures, procedure metrics, intellectual property, etc.
- **Public** - Applies to all other information which does not clearly fit into any of the above three classifications. Unauthorized disclosure isn't expected to seriously or adversely impact the company. Any release of this information must be authorized by GVSU PR Department.

PCI Requirements Reference:

Testing Procedure 9.6.1. Verify that all media is classified so the sensitivity of the data can be determined.

4.3 Data Access

All confidential or sensitive data must be protected via access controls to ensure that data is not improperly disclosed, modified, deleted or rendered unavailable. Logs must track all access to such data and identify who and when the data was accessed. See the *Logging Controls Policy (Section 16)* for more details.

Employees who have been authorized to view information at a particular classification level will only be permitted to access information at that level or at a lower level on a need to know basis. All

access to systems must be configured to deny all but what a particular user needs to access per their business role.

Access to systems or applications handling confidential, sensitive or private information must follow the data access request process. All requests require approval by the Information Technology Department and a valid *Authorization Request Form (Appendix G)* on file. Access to data exceeding the employee's authorized role must also follow the data access request process and must include documented limits around such access (e.g. access source, access time limits, etc.).

4.3.1 Data Access Request Process

The following generally describes the workflow used by GVSU for requesting new access:

1. The manager of the candidate (whether internal or external) will determine if they are fit to perform the new role and authorize access via the *Authorization Request Form (Appendix G)* by completing and signing the form. The form must reflect the access requirements based on the employee's role and clearly identify any additional access requirements above the standard defined role.

    a. The data owner department will determine if a formal background check for new employee is required.

2. The Information Technology Department will review the request and if the roles assigned to the employee are consistent with security policies, the form will be signed by a member of the Information Technology Department. If the access requested requires privileges above the user's role the Information Technology Department will engage additional system owners or management to collect approvals.

3. Once the Information Technology Department approves the request, they will forward it to the System Administrator for account creation.

4. The System Administrator will create the user account(s) requested.

5. The System Administrator will forward the completed request form to the HR Department for inclusion in the user's employee records and notify the Information Technology Department that the request has been completed.

Requests for change of access must be submitted by the user's manager utilizing the last version of the *Authorization Request Form (Appendix G)* on file.

Direction regarding removal of an employee's access shall follow the same workflow above except the request for removal can come from either the HR Department or the employee's manager.

4.4 Physical Security

Hard copy materials and electronic media containing confidential or sensitive information must be protected by appropriate physical access controls. In particular, the following must be observed:

- Cameras or other logged access control mechanisms must be used to monitor the entry and exit points of places where confidential or sensitive data is stored, processed or transmitted. Video cameras or other mechanisms should be protected from tampering or disabling. The data collected must be monitored and stored for at least 3 months unless otherwise restricted by law.

- Appropriate facility controls must be used to limit and monitor physical access to places where confidential or sensitive data is stored, processed or transmitted. Physical access to these places must be controlled with badge readers or similar technologies.
- Visitor logs and physical audit trails from access to sensitive areas must be collected and kept at least 3 months unless otherwise restricted by law. All visitor access must be recorded in the *Visitor Log (Appendix M).*
- Publicly accessible network jacks must be enabled only when needed by authorized personnel and disabled after use.
- Physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines must be restricted.
- Server consoles in the Data Center must be locked with user ID and password as per the *User Authentication Policy (Section 4.5)*.

PCI Requirements Reference:

Testing Procedure 9.1. Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment.

- Verify that access is controlled with badge readers or other devices including authorized badges and lock and key.
- Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.

Testing Procedure 9.1.1.a. Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas.

Testing Procedure 9.1.1.b. Verify that video cameras and/or access control mechanisms are protected from tampering or disabling.

Testing Procedure 9.1.1.c. Verify that video cameras and/or access control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.

Testing Procedure 9.1.2. Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and or logical controls are in place to restrict access to publicly accessible network jacks.

Testing Procedure 9.1.3. Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.

4.5 User Authentication

4.5.1 Users

Every user must use a unique user ID and a personal secret password for access to GVSU information systems and networks.

The use of non-authenticated (e.g. no password) user IDs or user IDs not associated with a single identified user are prohibited. Shared or group user IDs are prohibited.

Each user's access privileges must be: authorized according to business needs, restricted to least privileges necessary to perform job responsibilities and assigned based on job classification and function. Access control systems must have a default "deny-all" setting.

Additionally, if alternate authentication methods are used (Physical or logical security tokens, smart cards, certificates, etc.), they must be assigned to a single user and not shared among multiple

accounts. There must also be sufficient physical or logical controls in place so that only the intended account has access.

PCI Requirements Reference:

Testing Procedure 7.1.1. Select a sample of roles and verify access needs for each role are defined and included:

- System components and data resources that each role needs to access for their job function
- Identification of privilege necessary for each role to perform their job function.

Testing Procedure 7.2 Examine system settings and vendor documentation to verify that an access control system is implemented as follows:

Testing Procedure 7.2.1. Confirm that access control systems are in place on all system components.

Testing Procedure 7.2.2. Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.

Testing Procedure 7.2.3. Confirm that the access control systems have a default "deny-all" setting.

Testing Procedure 8.1.1

. Verify that all users are assigned a unique ID for access to system components or cardholder data.

Testing Procedure 8.1.2. For a sample of privileged user IDs and general IDs examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval.

Testing Procedure 8.4.a. Examine procedures and interview personnel to verify that authentication procedures and policies are distributed to all users.

Testing Procedure 8.4.b. Review authentication procedures and policies that are distributed to users and verify they include:

- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions for users not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised.

Testing Procedure 8.4.c. Interview a sample of users to verify that they are familiar with authentication procedures and policies.

8.5 Do not use group, shared, or generic accounts and passwords, or other authentication methods.

Testing Procedure 8.5.a. For a sample of system components, examine user ID lists to verify the following:

- Generic user IDs are disabled or removed.
- Shared user IDs for system administration activities and other critical functions do not exist.
- Shared and generic user IDs are not used to administer any system components.

Testing Procedure 8.5.b. Examine authentication policies/procedures to verify that use of group and shared ID's and/or other passwords or authentication methods are explicitly prohibited.

Testing Procedure 8.5.c. Interview system administrators to verify that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested.

Testing Procedure 8.6.a. Examine authentication policies and procedures to verify that procedures for using authentication mechanisms such as physical tokens, smart cards, and certificates are defined and include:

- Authentication mechanisms are assigned to an individual account and not shared among multiple accounts.

- Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.

Testing Procedure 8.6.b. Interview security personnel to verify authentication mechanisms are assigned to an account and not shared among multiple accounts.

Testing Procedure 8.6.c. Examine system configuration settings and/or physical controls, as applicable, to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access.

4.5.2 Systems

Each computer system shall have an automated or procedural access control process to authenticate all system users. The process must:

- Identify each User through a unique User identifier (user ID).
- Authenticate every user, system and application ID with a password.
- Require all passwords to be at least 7 characters in length.
- Require complex passwords, consisting of both numeric and alphabetic characters.
- Require that new passwords cannot be the same as the 4 previously used passwords.
- Lock out accounts after not more than 6 invalid logon attempts.
- Require that once a user account is locked out it remains locked for 30 minutes or until the System Administrator resets the account.
- Require system/session idle time set to 15 minutes (900 seconds).
- Require passwords to be reset at least once every 90 days. Note: Service level accounts (e.g. accounts that are not used interactively by users to login) may be exempt from this requirement with management approval. Administrative user IDs (e.g. root, system admin, database admin, etc.) must comply.
- Encrypt all passwords during transmission and storage on all system components (e.g. in scripts and databases, connection strings, inside compiled code, etc.).
- Remove or disable inactive users at least every 90 days.

PCI Requirements Reference:

Testing Procedure 8.1.6.a. For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than **six** invalid logon attempts.

Testing Procedure 8.1.7. For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of **30 minutes** or until a system administrator resets the account.

Testing Procedure 8.1.8. For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to **15 minutes** or less.

Testing Procedure 8.2. To verify that users are authenticated using unique ID and additional authentication (for example, a password) for access to the cardholder data environment, perform the following:

- Obtain and examine documentation describing the authentication method(s) used.
- For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).

Testing Procedure 8.2.1.a. Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage.

Testing Procedure 8.2.1.b. For a sample of system components, examine password files to verify passwords are unreadable during storage.

Testing Procedure 8.2.1.c. For a sample of system components, examine data transmissions to verify passwords are unreadable during transmission.

Testing Procedure 8.2.4.a. For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every **90 days**.

Testing Procedure 8.2.3.a. For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require at least the following strength/complexity:

- Require a minimum length of at least **7** characters
- Contain **both numeric and alphabetic** characters

Testing Procedure 8.2.5.a. For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the **four previously** used passwords.

4.6 Account and Access Management

4.6.1 Information Technology Systems Analysts

The Information Technology Systems Analysts will approve access authorization based on employees' job classification and function as discussed in the *Data Access Request Process (Section 4.3.1).*

The Information Technology Systems Analysts , in conjunction with business unit management, will maintain a role-based access control (RBAC) by defining the different roles and their minimum access levels. The *Access Control Matrix (Appendix Q)* must be used to document the RBAC.

A member of the Information Technology Systems Analysts must review the *Authorization Request Form (Appendix G)* to assure proper separation of duties.

The Information Technology Systems Analysts will perform a bi-annual audit of computer resource authorizations to confirm that access privileges are appropriate. The audit will consist of validating access rights for sample user populations (including a sample of privileged accounts). Also, a review of database application IDs must be included to verify that application IDs can only be used by the applications and not by individual users or other processes.

Extension authorizations for contractor accounts must go through the Information Technology Systems Analysts to provide an audit trail.

PCI Requirements Reference:

Testing Procedure 7.1. Examine written policy for access control and verify that the policy incorporates 7.1.1 through 7.1.4 as follows:

- Defining access needs and privilege assignments for each role.
- Restriction of access to privileged user IDs to least privilege necessary to perform job responsibilities.
- Assignment of access based on individual's personnel's job classification and function.
- Documented approval by authorized parties for all access, including listing of specific privileges approved.

Testing Procedure 7.1.1. Select a sample of roles and verify access needs for each role are defined and include:

- System components and data resources that each role needs to access for their job function.
- Identification of privilege necessary for each role to perform their job function.

Testing Procedure 7.1.2.a. Interview personnel responsible for assigning access to verify that access to privileged IDs is:

- Assigned only to roles that specifically require such privileged access
- Restricted to least privileges necessary to perform job responsibilities

Testing Procedure 7.1.2.b. Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are:

- Necessary for that individuals job function
- Restricted to least privilege necessary to perform job responsibilities

Testing Procedure 7.1.3. Select a sample of user IDs and interview responsible management personnel to verify privileges assigned are based on that individuals job classification and function.

Testing Procedure 7.1.4. Select a sample of user IDs and compare with documented approvals to verify that:

- Documented approval exists for the assigned privileges.
- The approval was by authorized parties.
- That specified privileges match the roles assigned to the individual.

Testing Procedure 8.7.d. Examine database access control settings, database application configuration settings, and the related applications IDs to verify that application IDs can only be used by the applications.

4.6.2 System Administrator Responsibilities

The System Administrator has the following responsibilities regarding user account and access management:

- Account creation requests must specify access either explicitly or via a "role" that has been mapped to the required access. The *Data Access Request Process (Section 4.3.1)* must be followed for the creation of new accounts.
- Access must be immediately revoked for terminated or transferred users or for any user whose access is no longer required. Ensure that access privileges are revoked as soon as possible by following the *Data Access Request Process (Section 4.3.1)*. Whenever possible validate employment using GVSU HR Department systems and immediately suspend users who are on leave-of-absence or extended disability.
- User IDs shall be removed or disabled after ninety (90) days of inactivity. This requirement may not apply to certain specialized accounts (e.g., admin, root, etc.). In those instances, the System Administrator must obtain a waiver to the Information Technology Department and document the additional security controls implemented to mitigate any risks associated with these User IDs.
- All computer resources capable of displaying a custom sign-on or similar message must display the following message as part of the login process:

```
This system is for the use of authorized users only. Individuals using
this computer system without authority, or in excess of their authority,
are subject to having all of their activities on this system monitored
and recorded by system personnel. In the course of monitoring individuals
improperly using this system, or in the course of system maintenance, the
activities of authorized users may also be monitored. Anyone using this
```

```
system expressly consents to such monitoring and is advised that if such
monitoring reveals possible criminal activity, system personnel may
provide the evidence of such monitoring to law enforcement officials.
```

- Passwords set by System Administrators must be changed by the user immediately upon the users' next login. System Administrators must set first-time passwords for new users, and reset passwords for existing users, to a unique value for each user and in compliance with the password rules.
- System Administrators must validate the identity of users before performing a password reset. The approved means for validating identity at GVSU is by doing it in person with a valid employee ID, or remotely by calling back the individual at a predetermined phone number. Remote validation can also be achieved by providing uniquely identifying pieces of information. Examples could include: employee ID, full name, date of birth, and home phone number.
- Contractor accounts must have Information Technology Department approval and must automatically expire at the end of the contract date. Extensions must be requested through the Information Technology Department. System Administrators must monitor these accounts carefully while they are in use.
- Vendor accounts used for remote maintenance must only be enabled during the time that access is needed and monitored while being used. The process described in *Remote Access (Section 8.4)* must be followed to connect and disconnect all external entities.
- Ensure that all systems and especially access to any databases containing cardholder data is authenticated (e.g., users, applications, administrators, etc.). All user activities on databases such as authentication, queries, or execution of commands like move, copy, and delete, must be done through programmatic methods or stored procedures only. User direct access or queries to database must be restricted to database administrators.
- System Administrators must enable audit logs to record user and administrative activities.
- Audit logs must be stored securely and retained according to the *Data Retention and Disposal Policy (Section 5.2).*
- Access to management consoles for wireless networks must be limited to the System Administrator. GVSU does not support wireless PCI networks.

PCI Requirements Reference:

Testing Procedure 2.2.2. Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, email, web, or other non-face-to-face method, the user's identity is verified before the password is reset.

Testing Procedure 8.1.2. For a sample of privilege user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval

Testing Procedure 8.1.3.a. Select a sample of employees terminated in the past six months, and review current user access lists to verify that their IDs have been deactivated or removed.

Testing Procedure 8.1.3.b. Verify all physical authentication methods such as smart cards, tokens, etc., have been returned or deactivated.

Testing Procedure 8.1.4. Verify that inactive accounts over 90 days old are either removed or disabled.

Testing Procedure 8.1.5.a. Interview personnel and observe processes for managing accounts used by vendors to access, support, or maintain system components to verify that accounts used by vendors for remote access are:

- Disabled when not in use
- Enabled only when needed by the vendor and disabled when not in use.

Testing Procedure 8.1.5.b. Verify that vendor remote access accounts are monitored while being used.

Testing Procedure 8.2.6. Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use.

Testing Procedure 8.7.a. Review database and application configuration settings and verify that all users are authenticated prior to access.

Testing Procedure 8.7.b. Examine database and application configuration settings to verify that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures).

Testing Procedure 8.7.c. Examine database access control settings and database application configuration settings to verify that user direct access to queries or databases are restricted to database administrators.

Testing Procedure 8.7.d. Examine database access control settings, database application configuration settings, and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).

Testing Procedure 10.1. Verify through observation and interviewing the system administrator, that:

- Audit trails are enabled and active for system components.
- Access to system components is linked to individual users.

5 DATA RETENTION AND DISPOSAL POLICY

5.1 Policy Applicability

All data deemed confidential or sensitive by the Information Technology Department which is stored on GVSU networks and systems must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

5.2 Retention Requirements

All confidential and sensitive data, regardless of storage location, will be retained only as long as required for legal, regulatory and business requirements. The specific retention length will be established by the data creator or Chief Information Security Officer.

As a special case, cardholder data used for single transactions may be kept for up to 4 days. This applies for cardholder data retained in any kind of format including digital and paper.

Cardholder data utilized for recurring transactions will be retained for the lifetime of the customer's account with GVSU. Once a customer's account is disabled or terminated, all the cardholder data for that account will be purged within 30 days of the termination using an approved destruction method. See the *Disposal Policy (Section 5.3)* for more details.

Cardholder "authentication data", including full track data (from the magnetic stripe on the back of a card or equivalent data on a chip), card verification code (CVV2, CVC2, CID, CAV2 data), and PINs and encrypted PIN blocks information, will be retained only until completion of the authorization of a transaction. After authorization, the data must be deleted according to the *Disposal Process Policy (section 5.4).* Storage of sensitive authentication data post-authorization is forbidden (even if encrypted).

All system and network audit logs must be retained for one year with the ability of immediately restoring at least the last three months' logs for analysis.

PCI Requirements Reference:

Testing Procedure 3.1.a. Examine the data retention and disposal policies, procedures and processes to verify they include at least the following:

- Legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data.
- Secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons.
- Coverage for all storage of cardholder data
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.

Testing Procedure 3.1.b. Interview personnel to verify that:

- All locations of stored cardholder data are included in the data retention and disposal processes.
- Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data.
- The quarterly automatic or manual process is performed for all locations of cardholder data.

Testing Procedure 3.1.c. For a sample of system components that store cardholder data:

- Examine files and system records to verify that the data stored does not exceed the requirements defined in the data retention policy.
- Observe the deletion mechanism to verify data is deleted securely.

Testing Procedure 3.2.c. For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization.

Testing Procedure 3.2.d. For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable.

***Note**: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:*

- There is a business justification
- The data is stored securely

Testing Procedure 3.2.1. For a sample of system components, examine data sources including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization:

- Incoming transaction data
- All logs (for example, transaction, history, debugging, error)
- History files
- Trace files
- Several database schemas
- Database contents

Testing Procedure 3.2.2. For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, and CAV2 data) is not stored after authorization:

- Incoming transaction data
- All logs (for example, transaction, history, debugging, error)
- History files
- Trace files
- Several database schemas
- Database contents

Testing Procedure 3.2.3. For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization:

- Incoming transaction data
- All logs (for example, transaction, history, debugging, error)
- History files
- Trace files
- Several database schemas
- Database contents

Testing Procedure 10.7.a. Examine security policies and procedures to verify that they define the following:

- Audit log retention policies
- Procedures for retaining audit logs for at least a year, with a minimum of three months immediately available online.

Testing Procedure 10.7.b. Interview personnel and examine audit logs to verify that audit logs are available for at least one year.

Testing Procedure 10.7.c. Interview personnel and observe processes to verify that at least the last three months' logs can be immediately restored for analysis.

5.3 Disposal Requirements

All confidential or sensitive electronic data, when no longer needed for legal, regulatory or business requirements must be removed from GVSU systems using an approved method documented in this policy. This requirement includes all data stored in systems, temporary files or contained on storage media.

All confidential or sensitive hardcopy data, when no longer needed for legal, regulatory or business requirements must be disposed by using an approved method documented in this policy. See the *Paper and Electronic Media Policies (Section 6)* for more details.

5.4 Disposal Process

For paper containing cardholder data, a review must be conducted at least on a quarterly basis, to verify that stored cardholder data does not exceed retention policy requirements.

Other applicable data stored in files and directories where the containing media will be re-used must be deleted securely by a "wiping" utility approved by the Information Technology Department.

Media containing confidential or sensitive data that should no longer be retained must be disposed of in a secure and safe manner as noted below:

- Hard disks: place in IT shred bins, sanitize (7-pass binary wipe) or physically incapacitate platters.
- Floppy disks: place in IT shred bins, disintegrate, incinerate, pulverize, shred or melt.
- Tape media: degauss, shred, incinerate, pulverize or melt.
- USB "thumb" drives, smart cards, and digital media: place in IT shred bins, incinerate, pulverize or melt.
- Optical disks (CDs and DVDs): place in IT shred bins, destroy optical surface, incinerate, pulverize, shred or melt.
- Hardcopies (paper receipts, paper reports, and faxes): cross-cut shredded, incinerated, or pulped.
- Swipe Terminals: place in IT shred bin, pulverize
- Dongles: place in IT shred bin, pulverize

Before computer or communications equipment can be sent to a vendor for trade-in, servicing or disposal, all confidential or sensitive information must be destroyed or removed according to the approved methods in this policy.

Removable computer storage media such as floppy, optical disks or magnetic tapes may not be donated to charity or otherwise recycled.

Outsourced destruction of media containing confidential or sensitive information must use a bonded Disposal Vendor.

Storage containers used for information to be destroyed (such as "to-be-shredded" containers) must be locked to prevent access to its contents.

PCI Requirements Reference:

Testing Procedure 3.1.a. Examine the data retention and disposal policies, procedures and processes to verify they include at least the following:

- Legal, regulatory, and business requirements for data retention, including specific requirements for retention of cardholder data.
- Secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons.
- Coverage for all storage of cardholder data
- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.

Testing Procedure 3.1.c. For a sample of system components that store cardholder data:

- Examine files and system records to verify that the data stored does not exceed the requirements defined in the data retention policy.
- Observe the deletion mechanism to verify data is deleted securely.

Testing Procedure 9.8. Examine the periodic media destruction policy and verify that it covers all media containing cardholder data and confirm the following:

- Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is no reasonable assurance the hard-copy materials cannot be reconstructed.
- Storage containers used for materials that are to be destroyed must be secured.
- Cardholder data on electronic media must be rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion), or by physically destroying the media.

Testing Procedure 9.8.1.b. Examine storage containers used for materials that contain information to be destroyed to verify that the containers are secured.

Testing Procedure 9.8.2. Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media).

6 PAPER AND ELECTRONIC MEDIA POLICIES

6.1 Policy Applicability

All employees handling hardcopy or electronic media must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

6.2 Storage

6.2.1 Physical Security

Hard copy materials and electronic media containing confidential or sensitive information must be protected by appropriate physical access controls as described in the *Physical Security Policy (Section 4.4)*.

6.2.2 Hardcopy Media

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

- Printed reports containing consumer confidential or sensitive data are to be physically retained, stored or archived only within secure GVSU office environments, and only for the minimum time deemed necessary for their use.
- At no time is printed material containing confidential or sensitive information to be removed from any GVSU Data Center without prior authorization from the Information Technology Department.
- All hardcopy material containing confidential or sensitive information should be clearly labeled as such.
- All confidential or sensitive hardcopy media must be stored in a secure and locked container (e.g. locker, cabinet, desk, storage bin) which has been approved by the Information Technology Department.
- Confidential or sensitive hardcopy material is never to be stored in unlocked or insecure containers or open workspaces.
- All confidential or sensitive hardcopy material sent outside the facility must be logged and sent via secured courier or other delivery method that can be accurately tracked and that has been approved by the Information Technology Department.

6.2.3 Electronic Media

Electronic media containing confidential or sensitive information (e.g., CD, DVD, floppy disk, hard disk, tape, USB "thumb" drive, etc.) is subject to the following storage guidelines:

- At no time is electronic media containing confidential or sensitive information to be removed from any GVSU Data Center without prior authorization from the Information Technology Department. This includes but is not limited to computer system backups.
- Electronic media containing consumer confidential or sensitive data are to be physically retained, stored or archived only within secure GVSU office environments, and only for the minimum time deemed necessary for their use.
- All electronic media containing confidential or sensitive information must be clearly labeled as such.

- All removable, confidential or sensitive electronic media must be stored securely.
- All confidential or sensitive electronic media sent outside the facility must be logged and sent via secured courier or other delivery method that can be accurately tracked and that has been approved by the Information Technology Department.

PCI Requirements Reference:

Testing Procedure 9.5. Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).

Testing Procedure 9.6. Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals.

Testing Procedure 9.6.2.a. Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be tracked.

Testing Procedure 9.6.2.b. Select a recent sample of several days of offsite tracking logs for all media and verify tracking details are documented.

Testing Procedure 9.6.3. Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals).

6.3 Payment Terminal Inventory

A *Media (Appendix D) and Capture Device (Appendix S) Inventory Log* is to be kept in all secure media (hardcopy and electronic) storage locations.

All stored electronic and hardcopy media containing confidential or sensitive information must be inventoried at least annually by the Information Technology Department. At this time, the security controls on the storage mechanism will be checked. Upon completion of the inventory the log will be updated.

The capture device Inventory Log must contain a list of all devices that capture payment card data (such as card swipe or dip). The Inventory log must contain at the minimum Make, model, location of device, and device serial number (or other method of unique identification). If mobile devices are used the location should be the person assigned to the device.

Ensure the list is updated anytime devices are added, relocated or no longer used.

If card payment capture devices are used, procedures to periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

The type and frequency of inspections is determined by the merchant, as defined by their annual risk-assessment process.

GVSU requires the following:

- Daily (or upon frequency of use) inspection of card-reading devices by department staff with inspection log sheets to be kept one full year within the department
- Monthly inspection of card-reading devices by department PCI Primary Contact with inspection log sheets to be kept one full year within the department

- Annual inspection by Business & Finance staff that maintain the annual log sheets for one full year and can be reviewed at the Business & Finance office in Zumberge Hall, Allendale, MI campus.

Ensure all card payment devices are inventoried annually and updated anytime devices are changed, or inspected (Appendix S).

All authorized wireless access points must be inventoried in Appendix T; the inventory entry for each authorized wireless access point must include a documented business justification.

PCI Requirements Reference:

Testing Procedure 9.7. Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.

Testing Procedure 9.7.1. Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually.

Testing Procedure 9.9. Examine documented policies and procedures to verify they include:

- Maintaining a list of devices
- Periodically inspecting devices to look for tampering or substitution
- Training personnel to be aware of suspicious behavior and to report tampering or substitution of devices.

Testing Procedure 9.9.1.a. Examine a list of devices to verify it includes:

- Make, model of device
- Location of device (for example, the address of the site or facility where the device is located).
- Device serial number or other method of unique identification.

Testing Procedure 9.9.1.b. Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up to date.

Testing Procedure 9.9.1.c. Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc.

Testing Procedure 9.9.2.a Examine documented procedures to verify processes are defined to include the following:

- Procedures for inspecting devices
- Frequency of inspections

Testing Procedure 9.9.2.b. Interview responsible personnel and observe inspection processes to verify:

- Personnel are aware of procedures for inspecting devices.
- All devices are periodically inspected for evidence of tampering and substitution.

Testing Procedure 11.1.1. Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points.

6.4 Destruction

Hardcopy and Electronic media must be destroyed as outlined in the *Data Retention and Disposal Policy (Section 5).*

All hardcopy shred bins must remain locked at all times (until shredding). Employees should make every effort to immediately cross-cut shred any printed material containing confidential or sensitive information.

7 FIREWALL AND ROUTER SECURITY ADMINISTRATION POLICY

7.1 Policy Applicability

All firewalls and routers on GVSU networks, whether managed by employees or by third parties, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

7.2 Device Management Responsibilities

Management of all GVSU firewalls and routers shall be a combined effort of the System Administrator and the Information Technology Department. The following subsections detail the responsibilities for these groups.

7.2.1 System Administrator

- Assure that changes to hardware, software, and security rules of firewalls and routers are approved by the Information Technology Department. Also, verify that all changes are performed as described in the *IT Change Control Policy (Section 3).*
- Document all firewall and router security rule changes utilizing the *Permitted Network Services and Protocols Form (Appendix F)*.
- Following every change, review and update network diagrams to assure they accurately describe all connections to confidential or sensitive information, wireless networks, and critical network protection mechanisms (e.g., firewalls, IDS/IPS, anti-virus systems, access control systems, etc.).
- Enable appropriate logging on all security systems and perform active daily monitoring of the logs that report security events.
- Report network security incidents to the Associate Director for Technical Services immediately upon discovery.
- Coordinate an appropriate response with the Information Technology Department to mitigate security events.
- Ensure that router configuration files are secured and synchronized properly. For example, running configuration files (used for normal running of the routers) and start-up configuration files (used when machines are re-booted), must have the same secure configuration.

PCI Requirements Reference:

Testing Procedure 1.2.2.a. Examine router configuration files to verify they are secured from unauthorized access

Testing Procedure 1.2.2.b. Examine router configuration files to verify they are synchronized. For example: The running or active configuration matches the start-up configuration (used when device is booted).

7.2.2 Information Technology Department

- Monitor system and application specific alerts on critical systems (e.g., interface up/down, firewall daemon failing, system reboots, etc.)
- Notify the appropriate parties in the event of a security system failure or security event.

- Assure that security rules applied to the firewalls and routers are sufficient to protect GVSU networks and corporate assets from external attacks and unauthorized access.
- Assure that security rules applied to the firewalls and routers are sufficient to prevent internal security events from leaving the GVSU network.
- Review all firewall and router security rule change requests for policy compliance prior to submission through the change management process.
- Ensure that all protocols/services allowed through the firewalls and routers are properly documented
- Ensure risky protocols, such as FTP, TELNET, POP3, IMAP, and SNMP, have undergone a risk assessment, have a current documented business need, and are secured as per documented security standard. For the PCI environment, these protocols must not be used or must be encrypted via SSH or other technology.
- Actively monitor firewall and router security events to identify internal or external security incidents.
- Conduct a review of all firewall and router rule sets according to the frequency specified in the *Configuration Review Policy, Section 7.5.*
- Coordinate an appropriate response with the System Administrator to mitigate security events.

PCI Requirements Reference:

Testing Procedure 1.1.5.a Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.

Testing Procedure 1.1.6.b. Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.

7.3 Allowed Services

The list of currently approved paths, services and ports, with their corresponding justifications, is listed in the *Permitted Network Services and Protocols Form (Appendix F)*. Every connectivity path and service that is not specifically permitted by this policy, with supporting documents issued by the Information Technology Department, must be blocked by GVSU firewalls by using an explicit or implicit "deny all" statement.

PCI Requirements Reference:

Testing Procedure 1.1.6.a. Verify that firewall and router configuration standards include a documented list of services, protocols and ports, including business justification for each—for example, hypertext transfer protocol (HTTP, Secure Shell (SSH), and Virtual Private Network (VPN) protocols.

Testing Procedure 1.2 Examine firewall and router configurations to verify that connections are restricted between untrusted networks and system components in the cardholder data environment, as follows:

Testing Procedure 1.2.1.a. Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment.

Testing Procedure 1.2.1.b. Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.

Testing Procedure 1.2.1.c. Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.

7.4 Allowed Network Connection Paths and Configuration Requirements

In order to restrict the connection paths, a firewall must be installed at each Internet connection and between any DMZ or wireless network and the internal network zone. In addition, the following must be followed:

All Internet-based inbound traffic is only permitted into a firewall segmented demilitarized zone (DMZ) network. In all cases, this traffic should be limited to only systems that provide authorized publicly accessible services, protocols and ports necessary for GVSU's business requirements.

Direct connections inbound or outbound are not allowed for traffic between the Internet and the internal PCI environment. All traffic must go through the DMZ.

Anti-spoofing technologies must be configured on perimeter devices, denying or rejecting all traffic with a:

- Source IP address matching internally allocated or GVSU owned address space.
- Source IP address matching RFC 1918 address space.
- Destination IP address matching RFC 1918 address space.

The use of a stateful packet inspection firewall must be utilized for Internet and wireless segmentation to only allow established connections into or out of each particular network segment.

VLANs with compliant ACLs may be used for internal PCI environment segmentation so long as the VLAN switch is compliant with PCI and hardened to prevent all currently identified switch exploits (e.g. ARP cache flood). If VLANs are used for segmentation, all applicable switches must comply with the firewall policy.

Databases must be located on an internal network which is segmented from the GVSU DMZ network and other untrusted networks.

Disclosure of private IP addresses and routing information from internal networks to the Internet must be prevented by using at least one of the following methods:

- Network Address Translation (NAT)
- Placing critical production servers behind proxy servers/firewalls or content caches
- Removal or filtering of route advertisements for private networks that employ registered addressing
- Internal use of RFC 1918 address space instead of registered addresses

PCI Requirements Reference:

Testing Procedure 1.1.4.a. Verify that firewall configuration standards include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.

Testing Procedure 1.1.4.b. Verify that the current network diagram is consistent with the firewall configuration standards.

Testing Procedure 1.2.3.a. Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment.

Testing Procedure 1.2.3.b. Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.

Testing Procedure 1.3. Examine firewall and router configurations, including but not limited to the choke router at the internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment.

Testing Procedure 1.3.1. Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.

Testing Procedure 1.3.2. Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ.

Testing Procedure 1.3.3. Examine firewall and router configurations to verify direct connections inbound or outbound are not allowed for traffic between the Internet and the cardholder data environment.

Testing Procedure 1.3.4. Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal address cannot pass from the Internet into the DMZ

Testing Procedure 1.3.5. Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.

Testing Procedure 1.3.6. Examine firewall and router configurations to verify that the firewall performs stateful inspection (dynamic packet filtering). (Only established connections should be allowed in, and only if they are associated with a previously established session.).

Testing Procedure 1.3.7. Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.

Testing Procedure 1.3.8.a. Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.

Testing Procedure 1.3.8.b. Examine firewall and router configurations to verify that any disclosure of private IP addresses and routing information to external entities is authorized.

7.5 Configuration Review

At least every 6 months, the Information Technology Department must thoroughly review each firewall and router rule set and record results of the review must be reported to the Associate Director of Technical Services.

PCI Requirements Reference:

Testing Procedure 1.1.7.a. Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.

Testing Procedure 1.1.7.b. Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months.

8 SYSTEM CONFIGURATION POLICY

8.1 Policy Applicability

All servers and network devices on GVSU networks, whether managed by employees or by third parties, must be built and deployed in accordance with this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Associate Director of Technical Services.

PCI Requirements Reference:

Testing Procedure 2.2.c. Examine policies and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network.

8.2 System Build and Deployment

8.2.1 System Purpose

All computing systems should be designated for a single primary purpose where possible (e.g., web servers, database servers, and DNS should be implemented on separate servers). For virtual environments, implement only one primary function per virtual system component. The host server in a virtual environment must also be configured following the system configuration policy.

PCI Requirements Reference:

Testing Procedure 2.2.1.a. Select a sample of system components and inspect the system configurations to verify that only one primary function is implemented per server.

Testing Procedure 2.2.1.b. If virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device.

8.2.2 System Configuration Standards

All systems, prior to deployment in the production environment must conform to the *System Configuration Standards (Appendix B)*. A valid business justification and risk assessment must exist for all deviations from GVSU published configuration standards. Deviations require email approval by the Associate Director of Technical Services and must be stored in the 'PCI Change Log' folder.

PCI Requirements Reference:

Testing Procedure **2.1.1.a. Interview responsible personnel and examine supporting documentation to verify that:**

- Encryption keys were changed from default at installation
- Encryption keys are changed anytime anyone with the knowledge of the keys leaves the company or changes positions.

Testing Procedure 2.1.1.b. Interview personnel and examine policies and procedures to verify:

- Default SNMP community strings are required to be changed upon installation.
- Default passwords/phrases on access points are required to be changed upon installation

Testing Procedure 2.1.1.c. Examine vendor documentation and login to wireless devices, with system administrator help, to verify:

- Default SNMP community strings are not used.
- Default passwords/passphrases on access points are not used.

Testing Procedure 2.1.1.d. Examine vendor documentation and observe wireless configurations settings to verify firmware on wireless devices is updated to support strong encryption for:

- Authentication over wireless networks.
- Transmission over wireless networks.

Testing Procedure 2.1.1.e. Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.

Testing Procedure 2.2.a. Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.

.

8.2.3 System Configuration Records

A *System Configuration Record (Appendix H)* must be completed for all deployed systems at the time of installation and kept on file for as long as the system is in service. This form must be updated with any future modifications to system configurations.

8.2.4 System Configuration Process

All new system deployments will follow this high level procedure:

1. Install operating system.
2. Update all operating system software per vendor recommendations.
3. Configure operating system parameters and secure the system according to the system configuration build documentation described in the *System Configuration Standards (Appendix B)*.
4. Install applications and software:
   a. Install system specific applications and software according to System Configuration Record (if this is a replacement for an existing system).
   b. Install applications and software necessary for the system's primary function.
5. Update all application software per vendor recommendations.
6. Configure application parameters according to the *System Configuration Standards (Appendix B)*.
7. Enable logging according to the *Logging Controls Policy (Section 16).*
8. Complete system specific *System Configuration Record (Appendix H)* and maintain on file.
9. Ensure that all vendor supplied defaults are changed before the system goes into production. For example, change all default passwords and simple network management protocol (SNMP) community strings, and eliminate all unnecessary accounts.
10. Verify that insecure protocols, services and demons, such as FTP, TELNET, POP3, IMAP, NetBIOS, and File Sharing are never used in the PCI environment or are protected using technologies like SSH, SFTP, or IPsec VPN. If any insecure protocols, services or demons are used, there must be a written justification and documentation of the security features used to compensate for the risk.
11. Configuring system security parameters to prevent misuse.

12. Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.

PCI Requirements Reference:

Testing Procedure 2.1.a. Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that **ALL** default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)

Testing Procedure 2.2.2.a. Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled.

Testing Procedure 2.2.2.b. Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards.

Testing Procedure 2.2.3.a. Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols.

Testing Procedure 2.2.4.a. Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components.

Testing Procedure 2.2.4.b. Examine the system configuration standards to verify that common security parameter settings are included.

Testing Procedure 2.2.4.c. Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards.

Testing Procedure 2.2.5.a. Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed.

Testing Procedure 2.2.5.b. Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration.

Testing Procedure 2.2.5.c. Examine the documentation and security parameters to verify that only documented functionality is preset on the sampled system components.

8.2.5 File Integrity Monitor (FIM) Tools

File integrity monitoring (FIM) tools must be used on all systems in the PCI environment to alert personnel to unauthorized modification of critical system files, configuration files, or content files. Unauthorized modifications may include changes, additions, and deletions of critical files.

FIM tools must be configured to perform critical file checks at least weekly.

The following files must be monitored:

- System executables
- Application executables
- Configuration and parameter files
- Centrally stored, historical or archived, log and audit files
- Additional critical files as determined through risk assessment or other means

For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating

system. Other critical files, such as those for custom applications, must be evaluated and defined by the Information Technology Department.

PCI Requirements Reference:

11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Note: *For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).*

Testing Procedure 11.5.a. Verify the use of a change-detection mechanism within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored:

- System executables
- Application executables
- Configuration and parameter files
- Additional critical files determined by entity (for example, through risk assessment or other means).
- Centrally stored, historical or archived, log and audit files

Testing Procedure 11.5.b. Verify the mechanism is configured to alert personnel to unauthorized modification of critical files, and to perform critical file comparisons at least weekly.

8.2.6 VPN Client and Personal Firewall Software

All computers and laptops used for remote access to the GVSU's network via the Internet must have the following software installed:

- GVSU Staff may only connect to the PCI Environment using the PCI-Jump Server using a GVSU Imaged Windows 10 or OS 10.10 Computer, which requires 2-Factor Authentication.
- Personal Firewall software with a non-user alterable configuration created by the Information Technology Department. This configuration will be implemented in the next image for January 2018. Compensating controls requires that changing configuration files is prohibited on any GVSU computer used to access the PCI environment.
- GVSU prohibits the use of mobile devices and/or employee-owned devices, including laptops, for remote access to the PCI environment or for any PCI processing unless device is approved and managed by GVSU IT.
- VPN Client software capable of supporting the company's 2-factor authentication solution.

PCI Requirements Reference:

Testing Procedure 1.4.a. Examine policies and configuration standards to verify:

- Personal firewall software is required for all mobile and/or employee-owned devices that connect to the Internet (for example, laptops used by employees) when outside the network, and which are also used to access the network.
- Specific configuration settings are defined for personal firewall software
- Personal firewall software is configured to actively run.

- Personal firewall software is configured to not be alterable by users of mobile and/or employee-owned devices.

Testing Procedure 1.4.b. Inspect a sample of mobile and/or employee-owned devices to verify that:

- Personal firewall software is installed and configured per the organization's specific configuration settings.
- Personal firewall software is actively running
- Personal firewall software is not alterable by users of mobile and/or employee-owned devices.

8.2.7 Anti-virus Software

All servers, workstations, and laptops utilizing an operating system commonly affected by viruses must have anti-virus software installed as described in the *Anti-virus Policy (Section 9).*

8.2.8 Time Synchronization

With the exception of the internal GVSU NTP (Network Time Protocol) servers, all GVSU production systems must be configured to use one of the internal NTP servers to maintain time synchronization with other systems in the environment. This must include any access monitoring equipment such as video cameras and logs created by key card controlled doorways.

At least 2 internal GVSU NTP servers will be configured to request time updates from the Internet sites time.nist.gov and time-nw.nist.gov. Client systems able to retrieve time settings from the internal NTP servers will be controlled by Access Control Lists (ACLs).

The NTP system will at all times be running the latest stable version of the software.

Any changes to the time synchronization configuration must be logged, monitored, and reviewed. Access to time data must be restricted to only personnel with a business need to access this data.

PCI Requirements Reference:

Testing Procedures 10.4 Examine configuration standards and processes **to** verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.

Testing Procedures 10.4.1.a. Examine the process for acquiring, distributing and storing the correct time within the organization to verify that:

- Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.
- Where there is more than one designated time server, the time servers peer with one another to keep accurate time.
- Systems receive time information only from designated central time server(s).

Testing Procedures 10.4.1.b. Observe the time-related system-parameter settings for a sample of system components to verify:

- Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC.
- Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time.
- Systems receive time only from designated central time server(s).

Testing Procedures 10.4.2.a. Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.

Testing Procedures 10.4.2.b. Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.

Testing Procedures 10.4.3. Examine system configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).

8.2.9 Cardholder Data Processing Applications

All GVSU applications dealing with the processing or retrieval of cardholder data must, where there is not a business need to display full primary account numbers (PAN), mask displayed PAN to no more than the first six (6) and last four (4) digits of the full PAN. If the application is designed for a specific purpose in which the full PAN must be displayed, approval must be given by the Information Technology Department. In all cases the application must limit the display of the full PAN to the fewest number of users possible.

PCI Requirements Reference:

Testing Procedure 3.3.a. Examine written policies and procedures for masking the display of PANs to verify:

- Incoming transaction data
- All logs (for example: transaction, history, or debugging)
- History files
- Trace files
- Several database schemas
- Database contents

Testing Procedure 3.3.b. Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests.

Testing Procedure 3.3.c. Examine displays of PAN (for example: on screen and paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see full PAN.

8.2.10 Cardholder Data Storage Applications

All GVSU applications or systems which store cardholder data must be configured in a manner which does not retain sensitive cardholder data such as full track data, card-verification codes, PINs or encrypted PIN blocks. See the *Data Retention and Disposal Policy (Section 5)* for more information on sensitive cardholder data. Storage devices on a network must be on an internal network segregated from the DMZ as described in *Allowed Network Connection Paths and Configuration Requirements (Section 7.4)*. All access to networked storage devices will have its authentication and communication encrypted. The PAN (Primary Account Number) must be rendered unreadable through one of the following:

- Strong one-way hash functions (hashed indexes) such as SHA-1 with salts.
- Truncation.
- Index tokens and pads (pads must be securely stored).
- Strong cryptography with associated key management processes and procedures. For more information, see the *Encryption Policy (Section 11.2.3)*.

In addition, the PAN must never be stored in clear text in databases, or removable media (such backup tapes). The PAN must not be written to audit logs. Also, if hashed and truncated versions of the same PAN are present anywhere in GVSU environment, additional controls should be in place to

ensure that the hashed and truncated versions cannot be correlated by unauthorized parties attempting to reconstruct the original PAN.

PCI Requirements Reference:

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures

Testing Procedure 3.4.a. Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable). Verify that the PAN is rendered unreadable using one of the following methods:

- One-way hashes based on strong cryptography
- Truncation
- Index tokens and pads, with the pads being securely stored
- Strong cryptography, with associated key-management processes and procedures.

Testing Procedure 3.4.b. Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).

Testing Procedure 3.4.c. Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable.

Testing Procedure 3.4.d. Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs.

Testing Procedure 3.4.e If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.

8.3 Vulnerability Identification and System Updates

8.3.1 Vulnerability Identification

Members of the Information Technology Department must be informed of information security issues and vulnerabilities applicable to GVSU computing systems. When security issues are identified, the Information Technology Department is responsible for notifying appropriate personnel, including System Administrators.

The primary method for identifying new threats as they arise will be through vendor and security specific Internet mailing lists. Although not complete, the following lists should be subscribed to as well as other vendor lists applicable to GVSU specific software packages and systems:

- CERT
- NT BUGTRAQ
- SANS

GVSU System Configuration Standards (Appendix B) must be updated to reflect measures required for protection from any newly discovered vulnerability.

In addition to identifying new vulnerabilities, members of the Information Technology Department need to assign a "risk rank" to all vulnerabilities applicable to the GVSU's environment. Rank

assignment should also take into account the criticality of the systems affected. Risk rank must be used to prioritize activities like patch installation and equipment upgrades.

The rank assigned to a patch or vulnerability needs to be based on industry best practices, such as the Common Vulnerability Scoring System, Version 2 (CVSSv2). In the case of CVSSv2, a vulnerability must be rated as "High" when it achieves a score of 4.0 or above. Also, vulnerabilities that are related to "SQL Injection" or "Cross-Site Scripting" need to be rated as high automatically. Where appropriate, risk rank should also be based on vendor classifications, where any issue described as "Critical", "Remote Code Execution" or "Exceptional", needs to be rated as a high risk. The evaluations of authoritative industry security sources should also be monitored, with any vulnerability that can lead to remote compromise added to the list as high risk.

PCI Requirements Reference:

Testing Procedure 2.2.b. Examine policies and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.2.

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high", "medium", or "low" to newly discovered security vulnerabilities.

Testing Procedure 6.2.a. Examine policies and procedures to verify that processes are defined for the following:

- To identify new security vulnerabilities
- To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities
- To use reputable outside sources for security vulnerability information

Testing Procedure 6.2.b. Interview responsible personnel and observe processes to verify that:

- New security vulnerabilities are identified.
- A risk ranking is assigned to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities.
- Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.

8.3.2 Vulnerability Testing

At least every quarter, the Information Technology Department must test for the presence of unauthorized wireless access points in all facilities by using a combination of: wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify any unauthorized wireless devices, including at least the following:

- WLAN cards inserted into system components
- Portable wireless devices connected to system components (for example, by USB, etc.)
- Wireless devices attached to a network port or network device

If automated monitoring is utilized (e.g. wireless IDS/IPS, NAC, etc.), the configuration must generate alerts to personnel. If at any point an unauthorized wireless device is suspected, GVSU's *Incident Response Plan (Section 14)* must be invoked and appropriate steps taken to deal with the possible consequences.

The Information Technology Department is responsible for conducting internal and external network vulnerability scans at least quarterly and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product

upgrades). The external vulnerability scan must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). External vulnerability scans conducted after network changes and all internal vulnerability scans may be performed by qualified internal personnel as long as they are organizationally separate from the management of the environment being tested. The results of each scan must satisfy the *AVS Program Guide Requirements* (e.g., no vulnerabilities rated higher than a 4.0 by the CVSSv2 and no automatic failures or any high vulnerabilities as defined in this policy).

Internal and external penetration tests at the network and application layer must be performed annually or after any significant change in the network. The network layer test should include components which support network functions as well as operating systems. Application layer test should include, at a minimum, the vulnerabilities listed in the *Secure Coding Guidelines (section 13.3.2).* If segmentation is used to isolate the cardholder environment or otherwise reduce scope penetration testing must include verification of segmentation controls. Penetration testing must test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

The Information Technology Department will coordinate the internal and external penetration tests utilizing a qualified security company or a qualified internal resource that has expertise in penetration testing or ethical hacking. If internal personnel are chosen to perform a penetration test, they must be organizationally separate from the management of the environment being tested. For example, the firewall administrator should not perform the firewall-penetration testing. All noted exploitable vulnerabilities must be corrected and testing repeated. All penetration tests must be performed following the guidelines published by the PCI Security Standard Council in the following information supplement:
https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf.

Networks and systems that fall under payment card system scope must also be monitored by an intrusion detection/prevention system (IDS/IPS) that alerts personnel of potential compromises and that is configured, maintained, and updated per vendor instructions to ensure optimal protection. The IDS/IPS must monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment.

All potential vulnerabilities identified through vulnerability scans and penetration tests will be documented in a formal report and communicated to appropriate personnel within GVSU for assessment and remediation. All vulnerabilities ranked "High" must be corrected utilizing the *Change Control Policy (Section 3)*. Follow up scans must be performed to confirm compliance with GVSU security standards.

The Chief Information Security Officer must coordinate an annual formal risk assessment process that identifies any existing or new threats and vulnerabilities to ensure GVSU assets are adequately protected. The risk assessment should be based on a mature methodology such as OCTAVE, ISO 27005 or NIST SP 800-30. The risk assessment must identify all critical assets, threats and vulnerabilities, and result in a formal, documented analysis of risk.

PCI Requirements Reference:

Testing Procedure 11.1.a. Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis.

Testing Procedure 11.1.b. Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components
- Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.)

- Wireless devices attached to a network port or network device

Testing Procedure 11.1.c. If wireless scanning is utilized, **e**xamine output from recent wireless scans to verify that:

- Authorized and unauthorized wireless access points are identified, and
- The scan is performed at least quarterly for all system components and facilities.

Testing Procedure 11.1.d. If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to personnel.

Testing Procedure 11.2. Examine scan reports and supporting documentation to verify that internal and external vulnerability scans are performed as follow:

Testing Procedure 11.2.1.a. Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.

Testing Procedure 11.2.1.b. Review the scan reports and verify that the scan process includes rescans until all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.

Testing Procedure 11.2.1.c. Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).

Testing Procedure 11.2.2.a. Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period.

Testing Procedure 11.2.2.b. Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures).

Testing Procedure 11.2.2.c. Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).

Testing Procedure 11.2.3.a. Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned.

Testing Procedure 11.2.3.b. Review scan reports and verify that the scan process includes rescans until:

- For external scans, no vulnerabilities exist that are scored greater than a 4.0 by the CVSS,
- For internal scans, all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.

Testing Procedure 11.2.3.c. Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).

11.3 Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented that includes the following:

- Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)
- Includes coverage for the entire CDE perimeter and critical systems
- Testing from both inside and outside network
- Includes testing to validate any segmentation and scope-reduction controls
- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5
- Defines network-layer penetration tests to include components that support network functions as well as operating systems
- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months
- Specifies retention of penetration testing results and remediation activities results.

Testing Procedure 11.3.1.a. Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows:

- Per the defined methodology
- At least annually
- After any significant changes to the environment

Testing Procedure 11.3.1.b. Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).

Testing Procedure 11.3.2.a. Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows. :

- Per the defined methodology
- At least annually
- After any significant changes to the environment.

Testing Procedure 11.3.3. Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.

Testing Procedure 11.3.4.a. Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.

Testing Procedure 11.3.4.b. Examine the results from the most recent penetration-testing methodology to verify segmentation controls:

- Is performed at least annually and after any changes to segmentation controls/methods.
- Covers all segmentation controls/methods in use.
- Verifies that segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.

Testing Procedure 11.4.a. Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic:

- At the perimeter of the cardholder data environment
- At critical points in the cardholder data environment

Testing Procedure 11.4.b. Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises.

Testing Procedure 11.4.c. Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.

Testing Procedure 12.2.a. Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.

Testing Procedure 12.2.b. Review risk assessment documentation to verify that the risk assessment process is performed at least annually and upon significant changes to the environment.

8.3.3 Security Patch Deployment

All security patches, hot-fixes and service packs identified by the Information Technology Department or the System Administrator, must be installed on applicable systems within 30 days of vendor release. Patch installation could be applied to less critical devices and systems within 3 months if approved by the Information Technology Department and based on a previous risk analysis. All installation of patches must follow the *IT Change Control Policy (Section 3).*

PCI Requirements Reference:

6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.

Note: *An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*

Testing Procedure 6.2.a. Examine policies and procedures related to security patch installation to verify processes are defined for:

- Installation of applicable critical vendor-supplied security patches within one month of release.
- Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months)

Testing Procedure 6.2.b. For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following:

- That applicable critical vendor-supplied security patches are installed within one month of release.
- All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months).

8.4 Remote Access

If access to any of the computing systems needs to be done remotely, adequate technologies must be used to guarantee that no risk is placed on GVSU network environment. In particular, the following must be followed:

- Technologies such as SSH, VPN or TLS v1.1 or higher must be used for all administration (even if done within the internal network).
- All remote access to the GVSU network involving public networks such as the Internet must be authenticated via a strong two-factor authentication scheme. This will be accomplished by using a password as one factor (something you know) and a unique token or certificate as the second factor (something you have).
- If there is a need to allow external access to a vendor or contractor, a maintenance window must be approved and scheduled ahead of time. The following process must be observed by the System Administrator to connect and disconnect external entities:
  - Verify that the *Management of Connected Entities Form (Appendix O)* has been properly completed and authorized by management before allowing any access.
  - In case of uncertainty, contact the manager authorizing the connection to verify the authenticity of the authorization.
  - Allow access at the appointed time.
  - Monitor connection.
  - Disable access after the allowed time is over.
  - Monitor system performance after the connection to identify any anomaly.

PCI Requirements Reference:

Testing Procedure 2.3. Select a sample of system components and verify that non-console administrative access is encrypted by performing the following:

Testing Procedure 2.3.a. Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested.

Testing Procedure 2.3.b. Review services and parameter files on systems to determine that Telnet and other insecure remote login commands are not available for non-console access.

Testing Procedure 2.3.c. Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography.

Testing Procedure 2.3.d. Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations.

Testing Procedure 8.3.a. Examine system configurations for remote access servers and systems to verify two-factor authentication is required for:

- All remote access by personnel
- All third-party/vendor remote access (including access to applications and system components for support or maintenance purposes).

Testing Procedure 8.3.b. Observe a sample of personnel (for example, users and administrators) connecting remotely to the network and verify that at least two of the three authentication methods are used.

9 ANTI-VIRUS POLICY

9.1 Policy Applicability

All in-scope systems, such as servers, workstations and laptops, which are commonly affected by viruses, whether managed by employees or by third parties, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

9.2 Software Configuration

All applicable systems must be configured with Information Technology Department approved anti-virus software. The anti-virus solution must be able to detect, remove and protect against all known types of malicious software such as viruses, Trojans, worms, spyware, adware, and rootkits. The software must be configured to receive automatic updates, perform periodic scans, log anti-virus events with routing to a central logging solution, and end users must not be able to configure or disable the software.

Anti-virus software, including the master installation of the software must be actively running at all times. In the event that there is a legitimate technical need to temporarily disable anti-virus solution for a specific purpose, it must be formally authorized by the Chief Information Security Officer on a case-by-case base for a limited time period. Additional security measures must be implemented for the period of time that anti-virus protection is not active if necessary to protect the system.

PCI Requirements Reference:

Testing Procedure 5.1. For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.

Testing Procedure 5.1.1. Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs;

- Detect all known types of malicious software
- Remove all known types of malicious software
- Protect against all know types of malicious software

(Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkit

Testing Procedure 5.1.2. Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software.
Testing Procedure 5.3.a. Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running.

Testing Procedure 5.3.b. Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by users.

Testing Procedure 5.3.c. Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for limited time period.

9.3 Signature Updates

All systems with anti-virus software must be configured to update virus signatures and scan engines on at least a daily basis.

9.4 Software Logging

Anti-virus software must alert the Information Technology Department in real-time to the detection of a virus as well as writing an entry to the centralized logging server.

The Information Technology Department will determine what steps to take based on the *Incident Response Policy (Section 14)*.

Retention of anti-virus software logs will be in accordance with the *Data Retention and Disposal Policy (Section 5).*

PCI Requirements Reference:

Testing Procedure 5.2.a. Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date.

Testing Procedure 5.2.b. Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are:

- Configured to perform automatic updates.
- Configured to perform periodic scans.

Testing Procedure 5.2.c. Examine a sample of system components including all operating system types commonly affected by malicious software, verify that:

- The anti-virus software and definitions are current.
- Periodic scans are performed.

Testing Procedure 5.2.d. Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that:

- Anti-virus software log generation is enabled
- Logs are retained in accordance with PCI DSS Requirement 10.7.

10 BACKUP POLICY

10.1 Policy Applicability

All system and application backups, whether performed by employees or by third parties, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

Note: No cardholder data is stored on GVSU computing resources, media or paper.

10.2 Location

The backup media for each of these systems is relocated to a secure off-site storage area.

The off-site storage location must be visited annually by management or a member of the Information Technology Department to confirm that it is physically secure.

PCI Requirements Reference

Testing Procedure 9.5. Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)

Testing Procedure 9.5.1.a. Observe the storage location's physical security to confirm that backup media storage is secure.

Testing Procedure 9.5.1.b. Verify that the storage location security is reviewed at least annually.

10.3 Transport

Offline storage media utilized for archival or back-up purposes must be handled and retained in a secured environment such that only GVSU personnel and contracted storage facility personnel have access to the archival media.

All media couriers and transport mechanisms must be certified by the Information Technology Department and they must be aligned with the *Paper and Electronic Media Policies (Section 6).*

Positive log-out and log-in of archive media will take place during all archive media transfers. All media that is transferred from one location to another should be logged as being transferred, by whom, where, and was it properly received, with signature from management. The *Backup Media Transfer Log (Appendix E)* must be used to document this process.

All media containing confidential or sensitive data must be classified and identifiable as such prior to transfer as detailed in the *Data Classification and Control Policy (Section 4).*

PCI Requirements Reference:

Testing Procedure 9.6.3. Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals)

10.4 Audit

All back-up media must be classified according to the *Data Classification Policy (Section 4.2)* and assigned a unique tracking number or similar feature that uniquely identifies the media. All media must be registered with the Information Technology Department for tracking prior to use.

Quarterly inventories of all stored media will take place. The Information Technology Department will compare their list of in-use media with records at the storage facility using the *Media Inventory Log (Appendix D)*.

10.5 Media Destruction

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 (Section 5).*

11 ENCRYPTION POLICY

11.1 Policy applicability

This policy documents encryption standards that must be used on all applicable mechanisms and systems on GVSU networks, whether managed by employees or by third parties. This policy also applies to the management of encryption keys which may be shared with customers to exchange confidential information. Documentation provided to customers who have a need to exchange encryption keys with GVSU must include these guidelines. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

11.2 Encryption Key Management

Data-encrypting keys and key-encrypting keys (a key that is used to encrypt a data-encrypting key) must be generated, accessed, distributed and stored in a controlled and secured manner.

PCI Requirements Reference:

Testing Procedure 3.6.3.a. Verify that key-management procedures specify how to securely store keys.

Testing Procedure 3.6.3.b. Observe the method for storing keys to verify that keys are stored securely.

11.2.1 Key Access

Encryption keys must be protected from general access. Only approved custodians should be able to access the key components.

Access to encryption key components will only be granted to those custodians specifically requiring access due to job function. Access may only be granted by the Chief Information Security Officer and key access must be noted on the matching *Authorization Request Form (Appendix G)*. Additionally, these users must sign the *Encryption Key Custodianship Form (Appendix I)* specifying that they understand their key custodian responsibilities. These forms will be maintained by the data owner department.

PCI Requirements Reference:

Testing Procedure 3.5.1. Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.

Testing Procedure 3.6.8.a. Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.

Testing Procedure 3.6.8.b. Observe documentation or other evidence showing that key custodians have acknowledged (in writing or electronically) that they understand and accept their key-custodian responsibilities.

11.2.2 Split Knowledge and Dual Control

If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control. For example, requiring two or three key custodians, each knowing only their own key component, to reconstruct the whole key. No single custodian may know or have access to all components of an encrypting key. Applicable key management operations include, but are not limited to: key generation, distribution, change, storage and destruction.

PCI Requirements Reference:

Testing Procedure 3.6.6.a. Verify that manual clear-text key-management procedures specify processes for the use of the following:

- Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND
- Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials (for example, passwords or keys) of another.

Testing Procedure 3.6.6.b. Interview personnel and/or observe processes to verify that manual clear-text keys are managed with:

- Split knowledge, AND
- Dual control

11.2.3 Key Generation

Only strong encryption keys are to be used. Creation of encryption keys must be accomplished using a random or pseudo-random number generation algorithm. Depending on the encryption scheme in question, the following are minimum length requirements for the encryption keys:

- AES (128 bits and higher)
- TDES (minimum double-length keys)
- RSA (2048 bits and higher)
- ECC (160 bits and higher)
- ElGamal (1024 bits and higher)
- Industry best practices for other industry-tested and accepted encryption methodologies. Example: NIST Special Publication 800-57 (http://csrc.nist.gov/publications/).

Generating encryption keys must be accomplished by a minimum of two custodians authorized by the Information Technology Department. Each custodian will generate one random clear text piece (key component) that will be used to create the encryption key.

To prevent unauthorized substitution of keys, physical and logical access to the key generating procedures and mechanisms must be secured.

PCI Requirements Reference:

Testing Procedure 3.6.1.a. Verify that key-management procedures specify how to generate strong keys.

Testing Procedure 3.6.1.b. Observe the method for generating keys to verify that strong keys are generated.

Testing Procedure 3.6.7.a. Verify that key-management procedures specify processes to prevent unauthorized substitution of keys.

Testing Procedure 3.6.7.b. Interview personnel and/or observe processes to verify that unauthorized substitution of keys is prevented.

11.2.4 Key Distribution

Only custodians authorized by the Information Technology Department are allowed to retrieve key components from secure storage or to distribute keys. Custodians must document all such actions in the *Encryption Key Management Log (Appendix J)*. The encryption keys must never be distributed in the clear.

PCI Requirements Reference:

Testing Procedure 3.6.2.a. Verify that key-management procedures specify how to securely distribute keys.

Testing Procedure 3.6.2.b. Observe the method for distributing keys to verify that keys are distributed securely.

11.2.5 Key Storage

All data-encrypting keys must be stored encrypted in a secure location and in the fewest number of possible locations and forms. Key-encrypting keys must be stored in physically and/or logically separate locations from data-encrypting keys. Even though there may be applications which need access to both keys, there must be sufficient access controls in place such that a human user does not have access to both the key-encrypting key and the encrypted data-encrypting key.

Clear-text backups of encryption key components must be stored separately in tamper-evident packaging in a secure location.

PCI Requirements Reference:

Testing Procedure 3.5.2.a. Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times.

- Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key
- Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)
- As key components or key shares, in accordance with an industry-accepted method

Testing Procedure 3.5.2.b. Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one (or more) of the following forms at all times.

- Encrypted with a key-encrypting key
- Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)
- As key components or key shares, in accordance with an industry-accepted method

Testing Procedure 3.5.2.c. Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify:

- Key-encrypting keys are at least as strong as the data-encrypting keys they protect
- Key-encrypting keys are stored separately from data-encrypting keys.

Testing Procedure 3.5.3. Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.

Testing Procedure 3.6.3.a. Verify that key-management procedures specify how to securely store keys.

Testing Procedure 3.6.3.b. Observe the method for storing keys to verify that keys are stored securely.

11.2.6 Key Changes and Destruction

An encryption key change is the process of generating a new key, decrypting the current production data and re-encrypting the confidential data with the new key.

All data-encrypting keys and corresponding key-encrypting keys must be changed regularly or when circumstances dictate a change to maintain encryption or key integrity. The following dictates when a key change is required:

- Regular Key Rotation: Keys must be changed at least every year.

- Suspicious Activity: Keys must be changed if they are known to be, or suspected of being, compromised.
- Resource Change: Keys must be changed if a resource with knowledge of a clear-text key terminates employment or assumes a new job role that no longer requires access to an encryption process.
- Technical Requirement: Keys must be changed if the key in place has become questionable due to a technical issue such as corruption or instability.

The Regular Key Rotation period (or crypto period) must be evaluated periodically to determine that it is still appropriate. This period could be determined by factors such as the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted. If provided by encryption application vendor, GVSU must follow the vendor's documented processes or recommendations for periodic changing of keys. The designated key owner or custodian can also refer to industry best practices on cryptographic algorithms and key management, for example NIST Special Publication 800-57, for guidance on the appropriate crypto period for different algorithms and key lengths.

Encryption keys no longer in service are to be disposed of in accordance with the process outlined in the *Data Retention and Disposal Policy (Section 5).* If old keys need to be kept (to support archived, encrypted data, for example) they should be strongly protected and used only for decryption/verification purposes.

PCI Requirements Reference:

Testing Procedure 3.6.4.a. Verify that key-management procedures include a defined crypto period for each key type in use and define a process for key changes at the end of the defined crypto period(s).

Testing Procedure 3.6.4.b. Interview personnel to verify that keys are changed at the end of the defined crypto period(s).

Testing Procedure 3.6.5.a. Verify that key-management procedures specify processes for the following:

- The retirement or replacement of keys when the integrity of the key has been weakened.
- The replacement of known or suspected compromised keys.
- Any keys retained after retiring or replacing are not used for encryption operations.

Testing Procedure 3.6.5.b. Interview personnel to verify the following processes are implemented:

- Keys are retired or replaces as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company.
- Keys are replaced if known or suspected to be compromised
- Any keys retained after retiring or replacing are not used for encryption operations.

11.3 Transmission over Un-trusted Networks

Confidential and sensitive information must be encrypted during transmission over networks in which is it easy and common for the data to be intercepted, modified or diverted (such as the Internet, wireless network, GSM, and GPRS). Some examples of strong encryption that is acceptable are:

- TLS ver. 1.1 or higher (ver. 1.2 highly recommended)
- Internet Protocol Security (IPSEC)
- SSH

The encryption technology used must only accept trusted keys and/or certificates, use secure configuration and not use insecure versions. The encryption strength must be strong and based on vendor recommendations or industry best practices.

Testing Procedure 4.1.a. Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations.

Testing Procedure 4.1.b. Review documented policies and procedures to verify processes are specified for the following:

- For acceptance of only trusted keys and/or certificates
- For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported)
- For implementation of proper encryption strength per the encryption methodology in use

Testing Procedure 4.1.c. Select and observe a sample of inbound and outbound transmissions as they occur to verify that all cardholder data is encrypted with strong cryptography during transit.

Testing Procedure 4.1.d. Examine keys and certificates to verify that only trusted keys and/or certificates are accepted.

Testing Procedure 4.1.e. Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations.

Testing Procedure 4.1.f. Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices

Testing Procedure 4.1.g. For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received.

For example, for browser-based implementations:

- "HTTPS" appears as the browser Universal Record Locator (URL) protocol, and
- Cardholder data is only requested if "HTTP" appears as part of the URL.

11.3.1 Email Transmission of Confidential Information

GVSU prohibits the sending of confidential and sensitive information through end-user messaging technologies such as e-mail, instant messaging, SMS or chat. Any exceptions must be authorized by the Information Technology Department and a strong encryption solution must be issued to protect the information.

PCI Requirements Reference:

4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).

Testing procedure 4.2.a. If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.

Testing procedure 4.2.b. Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.

11.3.2 Encryption of Wireless Networks

All wireless networks in use at GVSU facilities must be protected through secure data encryption such as IEEE 802.11i (WPA2), IPSEC VPN, TLS v1.2 or higher. Under no circumstances should the encryption strength be configured to be less than 128 bits.

Commented [A1]: TLS ver.1.1 can be used but requires additional configuration. Refer to NIST SP 800-52 rev 1 for guidance on secure TLS configurations.

PCI Requirements Reference:

4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

Note: *The use of WEP as a security control was prohibited as of 30 June 2010.*

Testing procedure 4.1.1. Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings to verify the following for all wireless networks identified:

- Industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission.
- Weak encryption (for example, WEP, SSL) is not used as a security control for authentication or transmission.

11.4 Disk Encryption

If disk encryption is ever used (rather than file or column-level database encryption), the following controls must be followed:

- Verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating systems mechanism.
- Verify that cryptographic keys are stored securely (e.g. stored on removable media that is adequately protected with strong access controls).
- Ensure that cardholder data on removable media is encrypted wherever stored. If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.

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 system or Active Directory accounts). Decryption keys must not be tied to user accounts.

Testing procedure 3.4.1.a. If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system's authentication mechanism (for example, not using local user account database or general network login credentials).

Testing procedure 3.4.1.b. Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).

Testing procedure 3.4.1.c. Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored.

Note: If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.

12 USAGE POLICY FOR CRITICAL TECHNOLOGIES

12.1 Policy Applicability

All users of critical technologies deployed on GVSU networks, whether employees, contractors or business partners must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

Critical technologies refers to the usage of the following technologies within the GVSU computing environment. This policy will be modified in the future to include any new critical technologies.

- Remote access technologies (VPN, or dial-in modem access).
- Wireless technologies.
- Removable electronic media (backup tapes, USB drives, external hard drives).
- Laptops.
- Tablets.
- Personal data/digital assistants (PDAs).
- E-mail usage.
- Internet usage.

12.2 Approval

The Information Technology Department must explicitly approve any use or deployment of critical technologies by job function, role or on an individual basis. These approvals must be documented on the user's *Authorization Request Form (Appendix G)*.

PCI Requirements Reference:

Testing procedure 12.3.1. Verify that the usage policies include processes for explicit approval from authorized parties to use technologies.

12.3 Authentication

User authentication mechanisms, where possible, must be integrated into the current GVSU authentication systems. Under no circumstances may the user authentication requirements be less strict than currently defined in the *User Authentication Policy (Section 4.5).*

All remote access to the GVSU network using these technologies must be authenticated via a strong two-factor authentication scheme approved by the Information Technology Department. See *Remote Access (Section 8.4)* for more details.

PCI Requirements Reference:

Testing procedure 12.3.2. Verify that the usage policies include processes for all technology use to be authenticated with user ID and password or other authentication item (for example, token).

12.4 Device Inventory

All approved critical devices must be noted on the *Critical Device Inventory (Appendix K)* by the Information Technology Department. Critical devices include, but are not limited to: computers,

laptops, tablets, PDAs, modems, wireless access points, and removable electronic media. All approved users of these technologies must be noted on the *Critical Device User List (Appendix L)*.

PCI Requirements Reference:

Testing procedure 12.3.3. Verify that the usage policies define a list of all devices and personnel authorized to use the devices.

12.5 Device Identification

All approved critical devices must be labeled with the device owner, contact information and device purpose.

PCI Requirements Reference:

Testing procedure 12.3.4. Verify that the usage policies define labeling of devices with information that can be correlated to owner, contact information and purpose.

12.6 Acceptable Use

Acceptable use of GVSU critical technologies is subject to the same guidelines and restrictions put forth in the *Security Awareness and Acceptable Use Policies (Appendix A)*.

PCI Requirements Reference:

Testing procedure 12.3.5. Verify that the usage policies define acceptable uses for the technology.

12.7 Permitted Locations

GVSU does not currently support any wireless Devices or Access Points in the PCI Environment.

PCI Requirements Reference:

Testing procedure 12.3.6. Verify that the usage policies define acceptable network locations for the technology.

12.8 Approved Products

Only Information Technology Department approved devices may be deployed into the GVSU network. The use of these devices must be logged according to the *Critical Device Inventory (Appendix K)* and *Critical Device User List (Appendix L).*

PCI Requirements Reference:

Testing procedure 12.3.7. Verify that the usage policies include a list of company-approved products.

12.9 Session Disconnect

All remote-access technologies must be configured to automatically disconnect sessions after 120 minutes of inactivity.

PCI Requirements Reference:

Testing procedure 12.3.8.a. Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.

Testing procedure 12.3.8.b. Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity.

12.10 Vendor Connections

All remote-access technologies and associated accounts used by vendor and business partners must be activated only when needed, with immediate deactivation after use. Activating these remote-access paths and accounts requires approval from the Information Technology Department or invoking established problem management procedures. Vendor maintenance accounts must follow the *Remote Access Policy (Section 8.4).*

PCI Requirements Reference:

Testing procedure 12.3.9. Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.

12.11 Cardholder Data Access

If cardholder data is available through remote-access technologies, special precautions must be taken. In particular, copying, moving, or storing cardholder data onto local hard drives and removable electronic media is prohibited. Personnel with a valid business need to see cardholder data must be authorized by the Information Technology Department and the data must be protected accordingly. The remote system accessing cardholder data must comply with all the GVSU security policies.

PCI Requirements Reference:

Testing procedure 12.3.10.a. Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.
Testing procedure 12.3.10.b. For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.

12.12 Approved Products

Only Information Technology Department approved devices may be deployed into the GVSU network. The use of these devices must be logged according to the *Critical Device Inventory (Appendix K)* and *Critical Device User List (Appendix L).*

PCI Requirements Reference:

Testing procedure 12.3.7. Verify that the usage policies include a list of company-approved products.

12.13 Session Disconnect

All remote-access technologies must be configured to automatically disconnect sessions after 30 minutes of inactivity.

PCI Requirements Reference:

Testing procedure 12.3.8.a. Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.

Testing procedure 12.3.8.b. Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity.

12.14 Vendor Connections

All remote-access technologies and associated accounts used by vendor and business partners must be activated only when needed, with immediate deactivation after use. Activating these remote-access paths and accounts requires approval from the Information Technology Department or invoking established problem management procedures. Vendor maintenance accounts must follow the *Remote Access Policy (Section 8.4).*

PCI Requirements Reference:

Testing procedure 12.3.9. Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.

12.15 Cardholder Data Access

If cardholder data is available through remote-access technologies, special precautions must be taken. In particular, copying, moving, or storing cardholder data onto local hard drives and removable electronic media is prohibited. Personnel with a valid business need to see cardholder data must be authorized by the Information Technology Department and the data must be protected accordingly. The remote system accessing cardholder data must comply with all the GVSU security policies.

PCI Requirements Reference:

Testing procedure 12.3.10.a. Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.
Testing procedure 12.3.10.b. For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.

13 SOFTWARE DEVELOPMENT POLICY

13.1 Policy Applicability

All development efforts of software designed to run on GVSU computing systems, whether managed by employees or by third parties, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

13.2 Development Environment

A test/development environment, separate from the production environment, must be used to test all new software (including patches). If the network has network connectivity with the production GVSU network, access controls must be in place to enforce the separation.

Separation of duties between personnel assigned to the test/development environments and those assigned to the production environment must be enforced by automated access controls.

Production data (real credit card numbers) will not be used for testing and development purposes. Test and development personnel must only use mock data (available from banks and card associations) on non-production systems and software.

All test data and test accounts must be removed before a system or application goes into production. Similarly, all custom application accounts, user IDs and passwords must be removed before an application goes into production or is released to end users.

All code promotion to the production environment will be performed by the System Administrators. Under no circumstances will the Software Development Department have full time read/write access to production applications or data. Under emergency situations developers may assist in troubleshooting utilizing an Emergency ID described in the *Information Technology Department Responsibilities (Section 4.6.1).*

PCI Requirements Reference:

Testing Procedure 6.3.1. Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user ID's and/or passwords are removed before an application goes into production or is released to customers.

Testing Procedure 6.4.1.a. Examine network documentation and network device configurations to verify that the development/test environments are separate from the production environment(s).

Testing Procedure 6.4.1.b. Examine access control settings to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s).

Testing Procedure 6.4.2. Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment.

Testing Procedure 6.4.3.a. Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) is not used for testing or development.

Testing Procedure 6.4.3.b. Examine a sample of test data to verify production data (live PANs) is not used for testing or development.

Testing Procedure 6.4.4.a. Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active.

Testing Procedure 6.4.4.b. Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active.

13.3 Secure Software Development Procedures

13.3.1 Development Life-Cycle

The software development life cycle at GVSU follows the industry recognized waterfall model for its software development life cycle.

Compliance with mandatory governmental and industry regulations (such as PCI-DSS) must be taken into consideration when developing new software applications. Security checks and control measures must be considered throughout the development life-cycle.

The high level overview of the security measures taking place within each phase of the GVSU development life cycle are as follows:

- **Requirements Analysis** – developers should determine whether application requirements are inherently insecure.
- **Design** – application components must be planned in a manner consistent with data and network security.
- **Development** – developers must consider all application vulnerabilities (i.e.: memory bound issues, privilege and access bypass, etc.).
- **Code Review** – the goal is to verify that code was developed according to the secure coding guidelines defined in this policy. A second developer, other than the originating code author, must conduct code reviews of all new and changed software, specifically in an attempt to identify security issues. The reviewer must be knowledgeable in code review and secure coding. All corrections must be implemented, and the code review results must be reviewed and approved by management prior to release. For all custom applications, code reviews must ensure that code is developed according to the *Secure Coding Guidelines (Section 13.3.2).*
- **QA Implementation** - implementation must not compromise security controls already in place, or introduce new vulnerabilities.
- **QA Testing** - in addition to functional and efficiency testing, all security features of the application must be tested.
- **Documentation** – all application feature and implementation documentation must include direction on proper security configurations.
- **Production Implementation** – implementation must not compromise security controls already in place, or introduce new vulnerabilities.
- **Production Testing** – in addition to functional and efficiency testing, all security features of the application must be tested.
- **Maintenance** – all future application maintenance should not compromise security controls already in place, or introduce new vulnerabilities. Any new code must be reviewed and tested as detailed above.

PCI Requirements Reference:

Testing Procedure 6.3.2.a. Examine written software-development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows:

Commented [A2]: Many organizations for which code development is a core activity will already have a documented SDLC policy. That policy can be incorporated into this section, or a reference to an external document can be inserted here. Every effort must be made to insure that there is a single authoritative source of policy, and that all personnel with responsibilities in this area know how to access those policies.

- Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices.
- Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5).
- Appropriate corrections are implemented prior to release.
- Code review results are reviewed and approved by management prior to release.

Testing Procedure 6.3.2.b. Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.

Testing Procedure 6.3.a. Examine written software development processes to verify that the processes are based on industry standards and/or best practices.

Testing Procedure 6.3.b. Examine written software development processes to verify that information security is included throughout the life cycle.

Testing Procedure 6.3.c. Examine written software development processes to verify that software applications are developed in accordance with PCI DSS.

13.3.2 Secure Coding Guidelines

All GVSU developers will receive training on secure coding practices. Internal and 3rd party development of proprietary software must utilize industry recognized security coding techniques to prevent common vulnerabilities. The following sources must be used:

- OWASP Guide (www.owasp.org)
- SANS CWE Top 25 (www.sans.org)
- CERT Secure Coding (www.securecoding.cert.org)

The following vulnerabilities must be considered during the Code Review and Testing phases for all applications:

- Injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.)
- Buffer overflow (Validate buffer boundaries and truncate input strings.)
- Insecure cryptographic storage (Prevent cryptographic flaws)
- Insecure communications (Properly encrypt all authenticated and sensitive communications)
- Improper error handling (Do not leak information via error messages)
- All "High" vulnerabilities as identified in the *Vulnerability Identification Policy (Section 8.3.1)*

The following vulnerabilities must be considered during the Code Review and Testing phases for all internal and external Web Applications

- Cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.)
- Improper Access Control, such as insecure direct object references, failure to restrict URL access, and directory traversal (Properly authenticate users and sanitize input. Do not expose internal object references to users.)
- Cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.)

Annually, and whenever significant modifications have taken place, all web-based applications will be put through an application-specific penetration test as described in *Vulnerability Testing (Section 8.3.2).*

In order to protect all public-facing web applications against known web-based attacks, at least one of the following methods must be used:

- At least annually or after any significant change, have all custom code for public-facing web applications reviewed by an organization (internal or external) that specializes in application security, and that is organizationally separate from the management of the application being reviewed. The application must be re-evaluated after the vulnerabilities are corrected. Manual or automated vulnerability security assessment tools or methods can be used.
- Utilize a web-application firewall in front of the public-facing web applications to detect, prevent web-based attacks, or generate an alert that is immediately investigated.

Note: *The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASPGuide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*

Testing Procedure 6.5.a. Examine software-development policies and procedures to verify that training in secure coding techniques is required for developers, based on industry best practices and guidance

Testing Procedure 6.5.b. Interview a sample of developers to verify that they are knowledgeable in secure coding techniques.

Testing Procedure 6.5.c. Examine records of training to verify that software developers received training on secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.

Testing Procedure 6.5.d. Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities.

Testing Procedure 6.5.1. Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include:

- Validating input to verify user data cannot modify meaning of commands and queries.
- Utilizing parameterized queries.

Testing Procedure 6.5.2. Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include:

- Validating buffer boundaries.
- Truncating input strings.

Testing Procedure 6.5.3. Examine software-development policies and procedures and interview responsible personnel to verify that insecure cryptographic storage is addressed by coding techniques that:

- Prevent cryptographic flaws.
- Use strong cryptographic algorithms and keys.

Testing Procedure 6.5.4. Examine software-development policies and procedures and interview responsible personnel to verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications.

Testing Procedure 6.5.5. Examine software-development policies and procedures and interview responsible personnel to verify that improper error handling is addressed by coding techniques that do not leak information via error messages (for example, by returning generic rather than specific error details).

Testing Procedure 6.5.6. Examine software-development policies and procedures and interview responsible personnel to verify that coding techniques address any "high risk" vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1.

Note: Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):

Testing Procedure 6.5.7. Examine software-development policies and procedures and interview responsible personnel to verify that cross-site-scripting (XSS) is addressed by coding techniques that include:

- Validating all parameters before inclusion
- Utilizing context-sensitive escaping

Testing Procedure 6.5.8. Examine software-development policies and procedures and interview responsible personnel to verify that improper access control, such as insecure direct object references, failure to restrict URL access, and directory traversal, is addressed by coding techniques that include:

- Proper authentication of users
- Sanitizing input
- Not exposing internal object references to users
- User interfaces that do not permit access to unauthorized functions

Testing Procedure 6.5.9. Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.

Testing Procedure 6.6. For public-facing web applications, ensure that either one of the following methods are in place as follows:

- Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed, using either manual or automated vulnerability security assessment tools or methods, as follows:
  - At least annually
  - After any changes
  - By an organization that specializes in application security
  - That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment
  - That all vulnerabilities are corrected
  - That the application is re-evaluated after the corrections
- Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows:
  - Is situated in front of public-facing web applications to detect and prevent web-based attacks.
  - Is actively running and up to date as applicable
  - Is generating audit logs
  - Is configured to either block web-based attacks, or generate an alert that is immediately investigated.

Note: *This assessment is not the same as the vulnerability scans performed for Requirement 11.2*

Note: "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.

13.3.3 Cardholder Data Processing Applications

All GVSU proprietary or custom applications dealing with the processing or retrieval of cardholder data must be designed in a manner which masks or truncates the displayed credit card number. If cardholder data is to be masked only the first 6 and last 4 digits may remain displayed *as per the*

System Configuration Policy (Section 8.2.9). If the application is designed for a specific purpose in which the full credit card number must be displayed, approval must be given by the Information Technology Department during the Requirements Analysis Phase as described in the *Software Development Policy (*Section *13.3.1)*. In all cases the application must limit the display of the full PAN to the fewest number of users possible.

14 INCIDENT RESPONSE PLAN AND PROCEDURES

14.1 Policy Applicability

All incident detections and responses, especially related to critical systems, must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

14.2 Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to:

- Theft, damage, or unauthorized access (e.g., unauthorized logins, papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Inaccurate information within databases, logs, files or paper records.
- Abnormal system behavior (e.g., unscheduled system reboot, unexpected messages, and abnormal errors in system log files or on terminals).
- Security event notifications (e.g., file integrity alerts, intrusion detection alarms, and physical security alarms).
- Detection of unauthorized wireless access points

All employees, regardless of job responsibilities, should be aware of the potential incident identifiers and who to notify in these situations. In all cases, every employee should report incidents per the instructions under *Reporting and Incident Declaration Procedures (Section 14.3)*, unless they are assigned other activities within the incident response plan.

14.3 Reporting and Incident Declaration Procedures

The Information Technology Department should be notified immediately of any suspected or real security incidents involving GVSU computing assets, particularly any critical system. If it is unclear as to whether a situation should be considered a security incident, the Information Technology Department should be contacted to evaluate the situation.

With the exception of steps outlined below, it is imperative that any investigative or corrective action be taken only by or under the oversight of the Information Technology Department personnel to assure the integrity of the incident investigation and recovery process. When faced with a potential situation you should do the following:

- **Preserve the evidence.** If the incident involves a compromised computer system, do not alter the state of the computer system. The following must be done:
  - Do not shutdown the computer or restart the computer.
  - Immediately disconnect the computer from the network by removing the network cable from the back of the computer.
  - The computer system should remain on and all currently running computer programs left as is.
- **Report the security incident.**

- Contact the Information Technology Department to report any suspected or actual incidents. The Information Technology Department's phone number should be well known to all employees and should page someone during non-business hours.
- No one should communicate with anyone outside of their supervisor(s) or the Information Technology Department about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the PR Department.
- Document any information you know while waiting for the Information Technology Department to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

- **Notification Process**
  - Once the Information Technology department is notified and an incident is confirmed, the Chief Information Security Officer should be immediately notified to begin the PCI Incident Response process
    - Chief Information Security Officer will notify appropriate IT security staff to engage in incident response
    - Chief Information Security Officer will notify members of the Financial and Information Security Team; University Communications, University Legal Team and appropriate departmental owner of area that the incident has occurred

14.4 Incident Severity Classification

The Information Technology Department will first attempt to determine if the security incident justifies a formal incident response.

In cases where a security incident does not require an incident response the situation will be forwarded to the appropriate area of IT to ensure that all technology support services required are rendered.

The following descriptions should be used to determine what response the Information Technology Department will take.

- **Level 1** - One instance of potentially unfriendly activity (e.g., finger, unauthorized telnet, port scan, corrected virus detection, unexpected performance peak, etc.).
- **Level 2** - One instance of a clear attempt to obtain unauthorized information or access (e.g., attempted download of secure password files, attempt to access restricted areas, single computer successful virus infection on a non-critical system, unauthorized vulnerability scan, etc.) or a second Level 1 attack.
- **Level 3** - Serious attempt or actual breach of security (e.g., multi-pronged attack, denial of service attempt, virus infection of a critical system or the network, successful buffer/stack overflow, successful unauthorized access to sensitive or critical data or systems, broken lock, stolen papers, etc.) or a second Level 2 attack.

Any Level 1 type incident occurring against systems storing confidential or sensitive data or originating from unauthorized internal systems is classified as a Level 2.

Any detection of an unauthorized wireless access point is to be assumed as a potential compromise of the cardholder data environment, and shall be responded to following the Special Response procedures in 14.5.2 below.

14.5 Incident Response

14.5.1 Typical Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls. The following actions should be taken by the Information Technology Department once an incident has been identified and classified.

14.5.1.1 Level 1

Contain and Monitor

- If possible, record the user, IP address and domain of intruder.
- Utilize approved technology controls to temporarily or permanently block the intruder's access.
- Maintain vigilance for future break-in attempts from this user or IP address.

14.5.1.2 Level 2

Contain, Monitor and Warn

- Collect and protect information associated with the intrusion.
- Utilize approved technology controls to temporarily or permanently block the intruder's access.
- Research the origin of the connection.
- Contact the Internet Service Provider (ISP) and ask for more information regarding the attempt and intruder.
- Research potential risks related to intrusion method attempted and re-evaluate for higher classification and incident containment, eradication, and recovery as described for Level 3 incident classifications.
- Upon identification, inform malicious user of our knowledge of their actions and warn of future recriminations if attempt is repeated. If an employee is the malicious user management should work with the HR Department to address the Acceptable Use violation appropriately.

14.5.1.3 Level 3

Contain, Eradicate, Recover and perform Root Cause Analysis

- If the incident involved cardholder data systems the Acquirer and applicable card associations must be notified. See the *Credit Card Compromise – Special Response (Section 14.5.2)* for more details.
- Contain the intrusion and decide what action to take. Consider unplugging the network cables, applying highly restrictive ACLs, deactivating or isolating the switch port, deactivating the user ID, terminating the user's session/change password etc.
- Collect and protect information associated with the intrusion via offline methods. In the event that forensic investigation is required the Information Technology Department will work with legal and management to identify appropriate forensic specialists.

- Notify management of the situation and maintain notification of progress at each following step.
- Eliminate the intruder's means of access and any related vulnerabilities.
- Research the origin of the connection.
- Contact the ISP and ask for more information regarding attempt and intruder, reminding them of their responsibility to assist in this regard.
- Research potential risks related to or damage caused by intrusion method used.

14.5.2 Credit Card Compromise – Special Response

For any incidents involving potential compromises of cardholder data, the Information Technology Department will use the following procedure:

- Contain and limit the exposure. Conduct a thorough investigation of the suspected or confirmed loss or theft of account information within twenty-four (24) hours of the compromise. To facilitate the investigation:
  - Log all actions taken (e.g., bound notebook, video camera, etc.).
  - Utilize chain of custody techniques during all transfers of equipment and information related to the incident.
  - Do not access or alter compromised systems (e.g., do not log on or change passwords; do not log in as ROOT).
  - Do not turn off the compromised machine. Instead, isolate compromised systems from the network (e.g., unplug the network cable, deactivate switch port, isolate to contained environment e.g. isolated VLAN). To preserve the evidence for a forensic investigation it is extremely important to not access the system. Use the *Critical Systems Restore Strategy (Section 14.8)* to reestablish critical business functions.
  - Preserve logs and electronic evidence.
  - If using a wireless network, change the SSID on the AP and other machines that may be using this connection (with the exception of any systems believed to be compromised).
  - Be on high alert and monitor all cardholder data systems.

- Alert all necessary parties. Be sure to notify:
  - Internal or External Incident Response Teams, if they are not already involved
  - Merchant bank
  - Local FBI Office
  - U.S. Secret Service (if Visa payment data is compromised)

- Follow appropriate procedures for each card association which GVSU utilizes for credit card services.

- **Visa.** Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed:

  http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf

- **MasterCard.** Contact your relationship manager or call the support line at 1-(636)-722-4100 for further guidance.
- **American Express.** Contact your relationship manager or call the support line at 1-(800)-528-5200 for further guidance.
- **Discover Card.** Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

- Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

PCI Requirements Reference:

Testing Procedure 12.10.1.a. Verify that the Incident Response Plan includes:
- Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum
- Specific incident response procedures,
- Business recovery and continuity procedures,
- Data back-up processes
- Analysis of legal requirements for reporting compromises (for example, California Bill 1386 which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database)
- Coverage and responses for all critical system components
- Reference or inclusion of incident response procedures from the payment brands

Testing Procedure 12.10.1.b. Interview personnel and review documentation from a sample of previously reported incident or alert to verify that the documented incident response plan and procedures were followed.

Testing Procedure 11.1.2.a. Examine the organization's incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected.

Testing Procedure 11.1.2.b. Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found.

14.5.3 Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Information Technology Department and all affected parties will meet to review the results of the investigation conducted under step 1, section 14.5.2 of this document to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly. Upon conclusion of the

investigation, systems will be restored to their non-compromised state in accordance with the *System Configuration Policy (Section 8)*.

PCI Requirements Reference:

Testing Procedure 12.10.6. Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

14.6 Plan Testing and Training

At least once a year, a mock-incident will be initiated to facilitate testing of the current plan. The exact incident to be tested will be at the discretion of the Information Technology Department. Once complete, a follow-up session, as detailed above in section 14.5.3, will be held.

All GVSU employees that could have an active role within incident response will be part of the test process.

Training regarding incident response responsibilities must be performed regularly to ensure employee's readiness for test and actual incidents.

PCI Requirements Reference:

Testing Procedure 12.10.2. Verify that the plan is tested at least annually.

Testing Procedure 12.10.4. Verify through observation, review of policies, and interviews of responsible personnel that staff with responsibilities for security breach response are periodically trained.

14.7 Automated Security System Notifications

All automated intrusion detection systems within the GVSU environment, including intrusion detection sensors and file integrity checking systems, will be configured to automatically notify the Information Technology Department of any potential compromises or attacks. Also, any automatic or manual detection of unauthorized wireless access points must trigger the Incident Response Plan.

A member of the Information Technology Department must be available on a 24/7 basis to initiate the incident response plan if warranted.

PCI Requirements Reference:

Testing Procedure 11.1.2.a. Examine the organization's incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected.

Testing Procedure 12.10.5. Verify through observation and review of processes that monitoring and responding to alerts from security systems, including detection of unauthorized wireless access points, are covered in the Incident Response Plan.

Testing Procedure 12.10.3. Verify through observation, review of policies, and interviews of responsible personnel, that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.

14.8 Critical Systems Restore Strategy

In case of an incident where critical systems used to perform normal operations are made unavailable due to an attack or a forensic investigation, the IT Department must guarantee that critical business functions continue with minimal impact until all systems are restored to normal operations.

15 EMPLOYEE IDENTIFICATION POLICY

15.1 Policy Applicability

All employees and visitors must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

Note: No cardholder data is stored on GVSU computing resources, media or paper.

15.2 Employee Requirements

Employees and visitors to GVSU facilities must, at all times, possess and clearly display ID badges. It is every employee's responsibility to keep watch for unknown persons or employees not displaying badges.

15.3 Facilities

The Information Technology Department must locate the badge creation system in a physically secure environment and access must be restricted to authorized personnel.

The building, datacenter and any other restricted areas must have a *Visitor Log (Appendix M)* in place. All visitors must sign the form, including: their name, firm represented, and the employee authorizing physical access (escort). This log must be retained for at least 3 months.

PCI Requirements Reference:

Testing Procedures 9.4. Verify that visitor authorization and access controls are in place as follows:

Testing Procedures 9.4.1.a. Observe procedures and interview personnel to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas where cardholder data is processed or maintained.

Testing Procedure 9.4.1.b. Observe the use of visitor badges or other identification to verify that a physical token badge does not permit unescorted access to physical area where cardholder data is processed or maintained.

Testing Procedure 9.4.2.a. Observe people within the facility to verify the use of visitor badges or other identification, and that visitors are easily distinguishable from onsite personnel.

Testing Procedure 9.4.2.b. Verify that visitor badges or other identification expire.

Testing Procedure 9.4.3 Observe visitors leaving the facility to verify visitors are asked to surrender their badge or other identification upon departure or expiration.

Testing Procedure 9.4.4.a. Verify that a visitor log is in use to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.

Testing Procedure 9.4.4.b. Verify that the log contains:

- The visitors name
- The firm represented
- The onsite personnel authorizing physical access

Testing Procedure 9.4.4.c. Verify that the log is retained for at least three months.

15.4 Badge Assignment Procedure

15.4.1 New Badges

The individual departments will notify the Information Technology Department as part of the new employee orientation process and provide a copy of the *Authorization Request Form (Appendix G)* signed by the new employee's direct manager.

The Information Technology Department will review requested access privileges and make a determination on whether to issue the badge as listed. If approved, the Information Technology Department will create and issue the badge to the new employee, with only approved access levels.

15.4.2 Visitor Badges

An access badge with no assigned access privileges is provided to visitors by the office receptionist upon request of the visited employee. These badges are clearly identifiable from assigned employee ID badges. The receptionist will place a date identifying the expiration on the badge (no longer than 1 day).

Employees may request to have a visitor badge assigned to allow access to certain areas. This request must be provided to the Information Technology Department at least one (1) day prior to the visit. In no cases may a visitor ID badge permit unescorted access to physical areas that store confidential data.

The receptionist must request the ID badge from the visitor at the end of the visit.

PCI Requirements Reference:

Testing Procedure 9.2.a. Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.

- Verify procedures include the following:
- Identifying new onsite personnel or visitors (for example, assigning badges)
- Changing access requirements
- Revoking terminated onsite personnel and expired visitor identification (such as ID badges)

Testing Procedure 9.2.b. Examine identification methods (such as ID badges) and observe processes for identifying and distinguishing between onsite personnel and visitors to verify that:

- Visitors are clearly identified
- It is easy to distinguish between onsite personnel and visitors

Testing Procedure 9.2.c. Verify that access to the identification process (such as a badge system) is limited to authorized personnel.

Testing Procedure 9.3.a. For a sample of onsite personnel with physical access to the CDE, interview responsible personnel and observe access control lists to verify that:

- Access to the CDE is authorized.
- Access is required for the individual's job function.

Testing Procedure 9.3.b. Observe personnel access the CDE to verify that all personnel are authorized before being granted access.

Testing Procedure 9.3.c. Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to the CDE.

Testing Procedure 9.3.3. Observe visitors leaving the facility to verify visitors are asked to surrender their ID badge upon departure or expiration.

15.4.3 Changing Access

All requests for a change in access level must be made directly to the Information Technology Department by the employee's direct manager. If the access request is approved, the Information Technology Department will make the modifications, create an updated *Authorization Request Form (Appendix G)* and provide the form to the HR Department for filing.

15.4.4 Revoking Badges

Upon being notified of an employee termination the Information Technology Department will immediately disable all badge accesses for the terminated employee.

The HR Department is responsible for collecting the badge from the terminated user, if possible.

PCI Requirements Reference:

Testing Procedure 9.3.c. Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to the CDE.

Testing Procedure 9.4.2.b. Verify that visitor badges expire.

Testing Procedures 9.2.a. Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors.

- Verify procedures include the following:
- Identifying new onsite personnel or visitors (for example, assigning badges)
- Changing access requirements
- Revoking terminated onsite personnel and expired visitor identification (such as ID badges)

16 SECURITY EVENT LOG MANAGEMENT

16.1 Policy Applicability

All users, administrators, applications and systems fall under this policy when performing their duties. Exemptions from this policy will be permitted only if approved in advance and in writing by the Associate Director of Technical Services.

16.2 Events Logged

Automated audit trails must be implemented for all system components to reconstruct the following events:

- All user access to cardholder data. GVSU does not store cardholder data.
- All administrative actions utilizing user IDs with significant privileges above a general user (e.g. root, user IDs with Administrator group privilege, etc.).
- Access to audit log files.
- Any user or administrator authentication attempts (both valid and invalid).
- Identification and authentication mechanism used.
- Initialization of audit log files.
- Creation or deletion of system-level objects (e.g. executables, libraries, configuration files, drivers, etc.).

PCI Requirements Reference:

Testing Procedures 10.2 Through interviews, examination of audit logs, and examination of audit log settings, perform the following:

Testing Procedures 10.2.1. Verify all individual access to cardholder data is logged.

Testing Procedures 10.2.2. Verify actions taken by any individual with root or administrative privileges is logged.

Testing Procedures 10.2.3. Verify access to all audit trails is logged.

Testing Procedures 10.2.4. Verify invalid logical access attempts are logged.

Testing Procedures 10.2.5.a. Verify use of identification and authentication mechanisms is logged.

Testing Procedures 10.2.5.b. Verify all elevation of privileges is logged.

Testing Procedures 10.2.5.c. Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.

Testing Procedures 10.2.6. Verify the following are logged:

- Initialization of audit logs
- Stopping or pausing of audit logs

Testing Procedures 10.2.7. Verify creation and deletion of system level objects are logged.

16.3 Event Log Structure

All system access event logs must contain at least the following information.

- User Identification.
- Type of event.

- Date and time of event.
- Result of the event (e.g. success or failure).
- Originating location of the event.
- The name of the affected data, system component or resource.

PCI Requirements Reference:

Testing Procedures 10.3 Through interviews and observation, for each auditable event (from 10.2), perform the following:

Testing Procedures 10.3.1. Verify user identification is included in log entries.

Testing Procedures 10.3.2. Verify type of event is included in log entries.

Testing Procedures 10.3.3. Verify date and time stamp is included in log entries.

Testing Procedures 10.3.4. Verify success or failure indication is included in log entries.

Testing Procedures 10.3.5. Verify origination of event is included in log entries.

Testing Procedures 10.3.6. Verify identity or name of affected data, system component, or resources is included in log entries.

16.4 Log Security

All event logs must be collected in a centralized location or media that is protected from unauthorized access and difficult to alter via access control mechanisms, physical segregation, and/or network segregation. The viewing of such logs is to occur on a need only basis. The logs will be further protected by a file integrity monitoring (FIM) system or a change-detection software that alerts the Information Technology Department upon unauthorized access or if existing log data is changed. Logs for external-facing technologies such as wireless, firewalls, DNS, and mail, must be copied onto a log server on the internal LAN.

PCI Requirements Reference:

Testing Procedures 10.5 Interview system administrator and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows:

Testing Procedures 10.5.1. Only individuals who have a job-related need can view audit trail files.

Testing Procedures 10.5.2. Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.

Testing Procedures 10.5.3. Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.

Testing Procedures 10.5.4. Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure centralized internal log server or media.

Testing Procedures 10.5.5. Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.

16.5 Log Review

Security event logs must be reviewed at least daily to identify anomalies or suspicious activity. Reviews must include:

- All security events
- Logs of all in-scope system components that store, process, or transmit CHD and/or SAD.
- Logs of , including, but not limited to: all critical system components
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)
    - All system components which store, process or transmit cardholder data
    - all servers and system components which perform security functions, including, but not limited to:

  Firewalls

All exceptions and anomalies identified during the review process, must be followed up on within the day and reported to the Associate Director for Technical Services by Email.

PCI Requirements Reference:

Testing Procedures 10.6.1.a Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools:

- All security events
- Logs of all system components that store, process, or transmit CHD and/or SAD
- Logs of all critical system components
    - Logs of all IDS/IPS sensors
    - Authentication servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers,
- E-commerce redirection servers, etc.)

Testing Procedures 10.6.1.b Observe processes and interview personnel to verify that the following are reviewed at least daily:

- All security events
- Logs of all system components that store, process, or transmit CHD and/or SAD
- Logs of all critical system components
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

Testing Procedures 10.6.2.a Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization's policies and as determined by the annual risk management strategy.

Testing Procedures 10.6.2.b Examine the organization's risk-assessment documentation and interview personnel to verify that reviews are performed in accordance with organization's policies and risk management strategy.

Testing Procedures 10.6.3.a Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process.

Testing Procedures 10.6.3.b Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed.

16.6 Log Retention

Audit trail history Security event logs must be retained for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup)..

PCI Requirements Reference:

Testing Procedures 10.76.1.a Examine security policies and procedures to verify that they define procedures are defined for reviewing the following:

- Audit at least daily, either manually or via log retention policies tools:

All security events
Logs of all system components that store, process, or transmit CHD and/or SAD
Logs of all critical system components
Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)

- **Testing** Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online.

Testing Procedures10.710.6.1.b Interview Observe processes and interview personnel and examine audit logs to verify that audit logs the following are retained for reviewed at least one year. Daily:

Testing Procedures10.7.c Interview personnel and observe processes to verify that at least the last three months' logs are immediately available for analysis.

All security events
Logs of all system components that store, process, or transmit CHD and/or SAD
Logs of all critical system components
Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

17 PAYMENT TERMINAL MANAGEMENT POLICY

17.1 Policy Applicability

All payment terminals or devices used to capture payment card data via direct physical interaction, including devices kept in reserve, are subject to this policy.

17.2 Inventory

GVSU will maintain an up-to-date list of payment terminals, to include, at a minimum, the following information:

- Make, model of device
- Location (address of the site or facility where the device is located)
- Device serial number or other method of unique identification

17.3 Physical Security

All devices that capture payment card data via direct physical interaction must be protected from tampering and substitution. GVSU will implement procedures to:

- Periodically inspect payment card devices for signs of tampering
- Periodically inspect payment card devices to ensure unauthorized substitutions have not occurred
- Ensure personnel are trained to be aware of suspicious behavior and detect attempted tampering or substitution of devices. Training, at a minimum, must include the following topics:
    - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.
    - Do not install, replace, or return devices without verification.
    - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices).
    - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer)

PCI Requirements Reference:

Testing Procedures 9.9 Examine documented policies and procedures to verify they include:

- Maintaining a list of Protect devices
- Periodically inspecting devices to look for that capture payment card data via direct physical interaction with the card from tampering or and substitution.
- Training personnel to be aware of suspicious behavior and to report tampering or substitution of devices.

Note: *These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*
Note: *Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.*
9.9 Examine documented policies and procedures to verify they include:
 Maintaining a list of devices

- Periodically inspecting devices to look for tampering or substitution
- Training personnel to be aware of suspicious behavior and to report tampering or substitution of devices.

18 THIRD PARTIES AND THIRD PARTY AGREEMENTS

18.1 Policy Applicability

This policy applies to all third parties which provide services to GVSU. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

18.2 Third Party Service Providers

For all third parties with whom cardholder data is shared or that could affect the security of the cardholder data environment (e.g., back-up tape storage facilities, managed service providers such as Web hosting companies or security service providers, those that receive data for fraud modeling purposes, or those that have incidental access to cardholder data or the cardholder data environment, such as providers of maintenance services), the following must be done:

- A list of all the third parties with whom cardholder data is shared or could affect the security of the cardholder data environment must be documented in the *List of Third Parties (Appendix R).*
- Before engaging any third parties, proper due diligence must be performed to ensure that the engagement does not negatively impact GVSU's PCI DSS compliance, by following the process described in the PCI SSC Information Supplement: Third-Party Security Assurance. This will be accomplished by following these steps:
  - Determine the scope of services to be provided by the service provider.
  - If the answers to any of the following are "Yes", the service provider is in scope for PCI DSS:
    - Will the service provider store, process or transmit cardholder data?
    - Will the service provider be involved in protection of or have access to cardholder data?
    - Will the service provider be involved in protection of or have access to the cardholder data environment?
    - Will the service provider have incidental access to the CDE?
  - If the service provider is in scope, the following due diligence must be performed:
    - Determine if the service provider has validated PCI DSS compliance for the specific services being requested. If not, determine if the service provider has evidence to prove the requested service meets the intent of PCI DSS requirements.
    - If it does, request validation documentation or evidence (e.g., ROC/AOC, dataflow diagram, network diagram)
    - If not, determine if the service provider has an ongoing project goal to become PCI DSS compliant, and request details of project plan/goals and timeframe to completion.
  - If requested documentation was provided, proceed with a risk assessment of the service provider; if not, a different service provider should be selected.
  - Payment card brands may maintain lists of validated third-party service providers that satisfy specific brand programs. Absence of a service provider on one of these lists does not mean that the service provider is not PCI DSS compliant, as many service providers choose to not be listed. Listing of a service provider on one of these

published lists does not provide complete assurance that the specific services applicable to GVSU's engagement with them are included in the validated service. Sufficient documentation must be obtained in order to provide assurance that all services applicable to GVSU's engagement with them are compliant.

- There must be a written agreement in place with all third-party service providers that includes an acknowledgement by the third party that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes or transmits on behalf of GVSU, or to the extent that they could impact the security of GVSU's cardholder data environment.
- At least once every year, the list of third parties described in the *List of Third Parties (Appendix R),* must be reviewed. A follow up with all third party service providers must be performed to monitor their PCI DSS compliance status, including obtaining current documentation, and to verify that the list of which PCI DSS requirements are maintained by GVSU and which are maintained by the service provider are still current.

PCI Requirements Reference:

Testing Procedure 12.8 Through observation, review of policies and procedures and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data (for example, backup storage facilities, managed service providers such as web-hosting companies or security service providers, those that receive data for fraud modeling purposes, etc.).

Testing Procedure 12.8.1. Verify that a list of service providers is maintained.

Testing Procedure 12.8.2. Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of cardholder data that the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

Testing Procedure 12.8.3. Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider.

Testing Procedure 12.8.4. Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.

Testing Procedure 12.8.5. Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

19 SERVICE PROVIDER RESPONSIBILITIES

19.1 Policy Applicability

This policy applies to all PCI services provided by GVSU to GVSU's customers. Exemptions from this policy will be permitted only if approved in advance and in writing by the Chief Information Security Officer.

19.2 Customer User Account Management

All customer user accounts must be protected. In particular the following must be followed:

- Passwords must be encrypted.
- Passwords must be at least 7 characters in length.
- Passwords are required to contain both numeric and alphabetic characters.
- New customer passwords cannot be the same as the previous four passwords.
- Customer accounts must be temporarily locked-out after not more than six invalid access attempts.
- Passwords must be changed periodically. Customers must be given guidance as to when, and under what circumstances, passwords must change.
- All the user account management details described in this section must be included in the *User Documentation* given to the customer.
- All customer user accounts which provide access to cardholder data must comply with all the requirements describes in section 8 of the PCI DSS. This document is available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

19.3 Shared Encryption Keys

If encryption keys are shared with customers for transmission of cardholder data, documentation must be provided to customers with guidance on how to securely store and change customer's encryption keys (used to transmit data between customer and GVSU).

19.4 Remote Access to Customer Premises

If GVSU is provided with remote access to customer premises, such as for support of POS systems or servers, a unique authentication credential (such as password/passphrase) must be used for each customer.

19.5 Shared Hosting Environments

All entities or customers' data hosted on shared hosting environments must be protected. In particular the following must be followed:

- Utilize unique credential for each client that is being managed.
- Ensure that each entity only has access to own cardholder data environment.
- If entities are allowed to run their own applications, these application processes must run using the unique ID of the entity. For example:

- No entity on the system can use a shared web server user ID.
- All CGI scripts used by an entity must be created and run as the entity's unique user ID.

- The user ID of application processes must not be a privileged user (root/admin).
- Each entity must have read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.). Also, an entity's files may not be shared by group.
- Entity's users must not have write access to shared system binaries.
- To ensure that each entity cannot monopolize server resources to exploit vulnerabilities (error, race, and restart conditions, resulting in, for example, buffer overflows), restrictions must be in place for the use of system resources such as Disk space, Bandwidth, Memory and CPU.
- Logging and audit trails must be enabled and unique to each entity's cardholder data environment and must be consistent with the *Logging Control Policy (Section 16).* Logs must be active by default and must be enabled for common third party applications.
- Logs must be available for review by the owning entity and the log locations must be clearly communicated to the owning entity.
- Viewing of log entries must be restricted to the owning entity.
- In the event of a compromise, a timely forensics investigation of related servers must be conducted according to the *Incident Response Plan and Procedures (Section 14).*

19.6 Storage of Sensitive Authentication Data

If sensitive authentication data is stored to issue credit cards, then a business justification needs to be documented and the data must be protected by encrypting it as per the *Encryption Policy (Section 11).*

Commented [A3]: If the organization is not an issuer and/or company that support issuing services and store sensitive authentication data, please remove this paragraph.

19.7 Service Provider Acknowledgement of Responsibility

Commented [A4]: This requirement applies only when the entity being assessed is a service provider.

An acknowledgement in writing shall be provided to all of GVSU's customers confirming GVSU will maintain all applicable PCI DSS requirements to the extent GVSU possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extend GVSU could impact the security of the customer's cardholder data environment.

PCI Requirements Reference for Service Providers:

Testing Procedure 2.6. Perform testing procedures A.1.1 through A.1.4 detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.

Testing Procedure 3.2.a. For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data.

Testing Procedure 3.6.a. Additional testing procedure for service provider assessments only: If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store and update customer's keys, in accordance with Requirements 3.6.1 through 3.6.8 below.

Testing Procedure 8.2.1.d. Additional testing procedures for service providers: observe password files to verify that customer passwords are unreadable during storage.

Testing Procedure 8.2.1.e. Additional testing procedures for service providers: Observe data transmissions to verify that customer passwords are unreadable during transmission.

Testing Procedure 8.2.4.b. Additional testing procedures for service providers: Review internal processes and customer/user documentation to verify that:

- **Non-**consumer user passwords are required to change periodically.
- **Non-**consumer users are given guidance as to when, and under what circumstances passwords must change.

Testing Procedure 8.2.3.b. **Additional testing procedures for service providers:** Review internal processes and customer/user documentation to verify that non-consumer user passwords are required to meet at least the following strength/complexity:

- Require a minimum length of at least seven characters.
- Contain both numeric and alphabetic characters.

Testing Procedure 8.2.5.b. Additional testing procedures for service providers: Review internal processes and customer/user documentation to verify that new non-consumer user passwords cannot be the same as the previous four passwords.

Testing Procedure 8.1.6.b. Additional testing procedures for service providers: Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.

Testing Procedure 8.5.1. Additional testing procedures for service providers: Examine authentication policies and procedures and interview personnel to verify that different authentication are used for access to each customer.

Testing Procedure 12.9. Additional testing procedure for service providers: Review service provider's policies and procedures and observe written agreement templates to confirm the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes or transmits the customer's cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer.

Note: *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*

APPENDIX A – SECURITY AWARENESS AND ACCEPTABLE USE POLICIES

Refer to the GVSU policies at www.gvsu.edu/policies for both the Security Awareness Policy and the Acceptable Use Policy. Both policies are required annually to be read and accepted by all employees performing PCI duties. Verification is done via the internal eDocuments process.

APPENDIX B – SYSTEM CONFIGURATION STANDARDS

Applicability

This appendix includes hardening and installation procedures for all off-the-shelf operating systems and applications used at GVSU. All installations of these operating systems and applications must adhere to these requirements.

B.1 Windows Systems

B1.1 Windows Installation

The following general install procedures will be followed for all GVSU Microsoft Windows-based system deployments:

1. Install operating system.
2. Update all operating system software per vendor recommendations.
3. Configure operating system parameters according to build document (OS hardening).
4. Install system specific applications and software according to a System Configuration Record, if one exists. Otherwise, install necessary software.
5. Update all application software per vendor recommendations.
6. Configure application parameters according to build document (application hardening).
7. Complete system specific *System Configuration Record and maintain (Appendix H)* on file.
8. Add notification listed in 4.6.2
9. A Detailed Functional description must be included in #Servers.

B.1.2 Windows Systems

The default desktop operating system for all new deployments at GVSU is Microsoft Windows 7.

Desktop systems will be configured in accordance with the policies detailed in:

https://benchmarks.cisecurity.org/tools2/windows/CIS_Microsoft_Windows_7_Benchmark_v1.1.0.pdf

For all other MS Windows systems, the system hardening documents located beneath the following link will be used as the basis for all GVSU system deployments:

http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.os.windows

While configuring the system, all exceptions to the appropriate hardening standard must be noted on the completed *System Configuration Record (Appendix H).*

B.2 UNIX Systems

B.2.3 Linux

The system hardening documents located beneath the following link will be used as the basis for all GVSU Linux network system deployments:

http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.os.linux

A specific guide to the Secure Configuration of Red Hat Enterprise Linux 5

http://www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed *System Configuration Record (Appendix H)*.

B.3 Network Devices

B.3.1 Network Device Installation –

The following general install procedures will be followed for all GVSU network device deployments:

1. Update all operating system or firmware software per vendor recommendations.
2. Configure device parameters according to build document (device hardening).
3. Disable unencrypted management interfaces (e.g. telnet) and enable encrypted management interfaces (SSH)
4. Complete system specific *System Configuration Record (Appendix H)* and maintain on file.

B.3.2 Cisco Devices

The system hardening documents located beneath the following link will be used as the basis for all GVSU Cisco IOS-based network system deployments:

Cisco Benchmark

http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.network.cisco

While configuring the system, all exceptions to this hardening standard must be noted on the completed *System Configuration Record (Appendix H)*.

While configuring the system, all exceptions to this standard must be noted on the completed *System Configuration Record (Appendix H)*.

B.4 Server Applications

B.4.1 Application Installation

The following general install procedures will be followed for all GVSU server application deployments:

1. Install necessary software.
2. Update application software per vendor recommendations.
3. Configure application parameters according to build document (application hardening).
4. Update system specific *System Configuration Record (Appendix H)* and maintain on file.

B.4.2 Oracle Database – GVSU does not use this for PCI

The system hardening documents located beneath the following link will be used as the basis for all GVSU Oracle database deployments:

Oracle Benchmark

http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.servers.database.oracle

While configuring the system, all exceptions to this hardening standard must be noted on the completed *System Configuration Record (Appendix H)*.

B.4.3 SQL Server 2014 – We don't use any SQL Servers for cardholder data, but to manage network configurations in PCI environment

The system hardening document located at the following link will be used as the basis for all GVSU SQL Server 2005 database deployments:

https://benchmarks.cisecurity.org/tools2/sqlserver/CIS_SQL2005_Benchmark_v1.2.0.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed *System Configuration Record (Appendix H)*.

B.4.5 Apache Web Server – We don't use any Web Servers in PCI

The system hardening document located at the following link will be used as the basis for all GVSU Apache web server deployments:

Apache Web Server

https://benchmarks.cisecurity.org/tools2/apache/CIS_Apache_HTTP_Server_Benchmark_v3.0.0.pdf

While configuring the system, all exceptions to this hardening standard must be noted on the completed *System Configuration Record (Appendix H)*.

B.4.6 Virtual Machines (e.g. VMWare)

The system hardening documents located beneath the following link will be used as the basis for all GVSU VMware virtual server deployments:

http://benchmarks.cisecurity.org/en-us/?route=downloads.browse.category.benchmarks.servers.virtualization.vmware

While configuring the system, all exceptions to this hardening standard must be noted on the completed *System Configuration Record (Appendix H)*.

APPENDIX C – CHANGE REQUEST FORM

The responsible party that will be implementing the change must complete and submit an email to the Associate Director of Technical Services (backup is the Chief Information Security Officer) which includes the following information:

- **Type of Request (new or update)**
- **Description of Change**
- **Requested implementation window**
- **Impact of change**
- **Back Out Plan**
- **Test Plan – which can be either a pre-test plan or a post-test validation.**
- **Approval will be via email reply and copied into the PCI Change Log folder along with the original request.**

GVSU Change Request Form

PART I (To be filled out by the Lead Requestor)		
1. Type of Request: □ Initial Request □ Updated Request	2. Office:	
3. Name (*Last, First, MI*):	4. Phone Number:	5. Date:
6. Type of Change: □ New Implementation □ Repair □ Removal □ Emergency □ Other _____		
7. Description of Change:		
8. Recurring Change: □ Yes, add to calendar □ No	9. Requested Implementation Window:	
10. Systems Affected by Change:	11: Users Affected by Change:	12. Documentation Attached: □ Test Plan □ Back out Plan
13. Resources That May be Affected by Change: □ Customer(s) □ Internal Dept. □ Other Explain _____	14. Criticality of Change: □ High □ Medium □ Low Explain _____	
PART II (To be completed by Management)		
15. Review Date:	16. Review Participants:	
17. Test Plan Review: □ Acceptable □ Further Action is Required	18. Back Out Plan Review: □ Acceptable □ Further Action is Required	

19. Resource Review:	20. Schedule Review:
□ Acceptable □ Further Action is Required	□ Acceptable □ Further Action is Required
21. Comments:	
PART III (To be completed by Management after approval)	
22. Approval Date:	23. Approved Implementation Date:
24. Supervising Official Certification:	
Name Phone Signature Date	
_____ _____ _____ _____	

APPENDIX D – MEDIA INVENTORY LOG

GVSU Media Inventory Log

GVSU prohibits cardholder data from being stored on any media device

Date	Location	Name	Signature	Acceptable
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No
				□ Yes □ No

APPENDIX E – BACKUP MEDIA TRANSFER LOG

GVSU Media Transfer Log

Date	Container #	Courier Signature	Management Signature

APENDIX F – PERMITTED NETWORK SERVICES AND PROTOCOLS

Firewall	Source	Destination	Ports	Protocols	Business Justification
PCI Firewall	Internet	No access allowed, only reflexive			
PCI Firewall	Internal	Payment Providers	80, 443	HTTP, HTTPS	Hosted order pages
PCI Firewall	Tech Support net 69-70	PCI-JUMP	3389	RDP	Administrator Access

APPENDIX G – AUTHORIZATION REQUEST FORM

GVSU requires each department to approve and manage account access.

GVSU has approved the following equipment for PCI use:

- **GVSU PCI compliant computers provided by GVSU IT**
- **NCR Silver Mobile checkout using cellular service**
- **Elavon Converge**
- **GVSU provided swipe terminals**
- **PCI compliant 3rd party vendor solutions approved by GVSU IT**
- **GVSU Hosted Order Page handing off to Cybersource**
- **Dedicated PO box**

Request and approval processes are managed via email. For further information, see dfs\Tech-Support-Data\IT-DIRECTOR-PCI\Inventory\PCI Owner List.xlsx

Authorization Request Form

Commented [A5]: This form is not used by GVSU.

PART I (To be filled out by the Requestor or Requestor's Supervisor)			
1. Type of Request: ☐ Initial ☐ Modification ☐ Deletion		2. Office:	
3. Name (*Last, First, MI*):		4. Title:	
5. Organization:	6. Phone Number:	7. Start Date:	8. Stop Date:
9. Requestor's Signature:			10. Date:

PART II (To be filled out by the Requestor's Supervisor)

11. Role (Must use a role defined in Appendix Q):

☐ Basic User ☐ System Administrator ☐ Support ☐ Key Custodian

☐ Manager ☐ Security Administrator ☐ Developer ☐ Other _____

Commented [A6]: Update this based on the role information detailed in Appendix Q.

12. ID Badge:		13. Equipment Assigned and Miscellaneous Access:		
☐ Visitor	☐ Building	☐ Workstation	☐ E-mail Use	☐ Modem Use
☐ Internal Doors	☐ Datacenter	☐ Laptop	☐ Internet Use	☐ Wireless Use
		☐ PDA	☐ VPN Access	☐ Removable Media

Commented [A7]: This is the equipment and access to technology that different users may have to perform their daily duties. Update the list as needed.

14. Justification for Accesses:

15. Supervising Official Certification:

Name	Phone	Signature	Date
_____	_____	_____	_____

PART III (To be completed by the HR Department)

16. Background Check Completed: ☐ Yes ☐ No	17. Performed By:	18. Date Granted:
19. HR Department Official Certification: Name Phone Signature Date _____ _____ _____ _____		
PART IV (To be completed by Information Technology Department)		
20. User ID:	21. Date User Notified:	22. Date Deleted:
23. Information Technology Department Official Certification: Name Phone Signature Date _____ _____ _____ _____		
Notes		
24. Additional Comments / Notes:		

APPENDIX H – SYSTEM CONFIGURATION RECORD

Current Configuration are tracked in #Servers.xlsx #IPAddresses.xlsx and PCI Inventory.xlsx

Configuration Changes are tracked in the PCI Change Log Outlook Folder.

GVSU System Configuration Record

General System Information		
1. System Name:	2. System Purpose:	3. Build Date:
4. Build Engineer:	5. Comments:	
IP Information		
6. IP Address:	7. Subnet Mask:	8. Default Gateway:
9. DNS/WINS Entries:	10. Domain:	11. Other Settings:
Operating System		
12. Operating System:	13. Version:	
14. Date Patched to:	15: Patch Exceptions:	
16. System Hardened: □ Yes □ No	17. Hardened by Which Standard:	
18. Hardening Exceptions: Document Number Reason for Exception _____ _____		
Application (Attach additional Sheets for Other Entries)		
19. Operating System and Applications	20. Version:	
21. Date Patched to:	22: Patch Exceptions:	
23. System/application Hardened: □ Yes □ No	24. Hardened by Which Standard:	
25. Hardening Exceptions: Document Number and Reason for Exception _____ _____		
Notes		

26. Additional Comments / Notes:

APPENDIX I – ENCRYPTION KEY CUSTODIANSHIP FORM

GVSU does not store cardholder data and does not use shared encryption keys.

GVSU Encryption Key Custodianship Form

Encryption key custodians are those person(s) delegated the responsibility of managing, handling and protecting access to GVSU encryption keys. Custodians are responsible for the confidentiality and integrity of key components in their custody. In particular, the custodian has responsibility to:

- Implement all encryption key controls as specified by the Information Technology Department and documented in information security policies and procedures.
- Provide safeguards for encryption keys during generation, loading and storage.
- Administer access to the encryption keys and make provisions for timely detection, reporting, and analysis of unauthorized attempts to gain access to these keys.
- Control access and secrecy of the combination of the safe containing the clear-text encryption keys.
- Complete the Encryption Key Management Log for any activity involving cryptographic keys.
- Participation in the encryption key generation, distribution, change, and destruction processes.

By signing this form I acknowledge that I understand and accept of my responsibilities as key custodian.

_____ _____

Key Custodian Signature Date

_____

Printed Name

APPENDIX J – ENCRYPTION KEY MANAGEMENT LOG

GVSU does not store cardholder data and does not use shared encryption keys.

GVSU Encryption Key Management Log

Date	Time	Key	Custodian and Witness	Reason

APPENDIX K – CRITICAL DEVICE INVENTORY

GVSU Critical Device Inventory

Refer to below locations for Device Inventory:

\\office.ads.gvsu.edu\dfs\Tech-Support-Data\PCI\Inventory

and

\\office.ads.gvsu.edu\dfs\Tech-Support-Data\IT-DIRECTOR-PCI\Inventory\GVSU PCI Application List

Type	Vendor / Model	Device Name	Location	Owner / Administrator

APPENDIX L – CRITICAL DEVICE USER LIST

GVSU Critical Device User List

Refer to below locations for Device User List:
\\office.ads.gvsu.edu\dfs\Tech-Support-Data\PCI\Inventory
and

\\office.ads.gvsu.edu\dfs\Tech-Support-Data\IT-DIRECTOR-PCI\Inventory\GVSU PCI Application List

Device Name	User	Justification / Restrictions

APPENDIX M – VISITOR LOG

GVSU restricts the PCI server environment to two card access racks with logging.

GVSU Visitor Log

Date	Time In	Visitor's Name	Visitor's Company	Access Authorized by (Employee's Name)	Time Out

APPENDIX N – PERIODIC OPERATIONAL SECURITY PROCEDURES

BF-Jim BF-Kyle BF-Greg BF-Sue

GVSU Periodic Operational Security Procedures

Task	Daily	Weekly	Quarterly	Bi-Annual	Annually	Target Window
Security Policy						
Verify the scope of the PCI Environment					Bill/Sue	Q1
Enterprise Risk Analysis					Sue to report to FIST	Q1
Policy/standards review					Bill/Sue	Q1
Security awareness orientation					Sue	Q1
Organizational Security						
Review security policy exceptions compliance					Bill	As needed
Verify PCI DSS compliance status of third parties					Sue	Q1
Test Incident Response Plan					Bill/Sue/Greg +	Q2
Asset Classification and Control						
Review system access controls				Bill		Q1 and Q3
Review access request approvals & audit trail				Analysts		Q1 and Q3
Audit disposal of data and media (including hardcopy)			Sue/Users			Jan/Apr/Jul/ Oct
Personnel Security						
Audit terminated employee samples for system, network, application access			Sue/Analysts			Jan/Apr/Jul/ Oct
Incident response team meeting					Bill/Sue/Greg	As needed
Physical and Environmental Security						
Visit offsite storage facility and perform media inventory					NA	
Review compliance of Data Center access & visitor logs					Jim	Q1
System Security						
File Integrity Scan	Jason					
Review intrusion detection (IDS/IPS) logs	Greg					
Review all other security and event logs	Yvonne /Greg					
External vulnerability scan			3rd party			Jan/Apr/Jul/ Oct
Internal vulnerability scan			Luke/Greg			Jan/Apr/Jul/ Oct
Use a Wireless Analyzer to detect unauthorized wireless devices in use			Kyle			
Firewall rule set review				Ben/Jim		Jan/Apr/Jul/ Oct
External penetration testing					3rd party	Q1
Internal penetration testing					3rd party	Q1

Data encryption key rotation					NA	
Review of outside vulnerability sources (notifications from CERT, NT BUGTRAQ, SANS)					Greg	As needed
Handheld Terminal review	Depts	Supervisor	SK		Bus&Fin	

Commented [A8]: This list should match the list in Section (Vulnerability Identification Policy)

APPENDIX O – MANAGEMENT OF CONNECTED ENTITIES FORM

Commented [A9]: This form is used to meet requirement 8.3 and 8.5.6. Keep this in mind and check all references to this appendix before you remove it.

GVSU does not allow connected entities to the PCI environment

Company Name	Connection type and accessed system	Requested connection date	Requested connection time	Reason	Authorized by Manager/Title	Time Out

APPENDIX P – PCI ENVIRONMENT DESCRIPTION

This section defines the scope of the Payment Card Industry Data Security Standards (PCI DSS) within GVSU network environment. All the policies and procedures within this document must be followed within the cardholder environment to maintain compliance with the PCI DSS. Any deviation may put GVSU in a dangerous position by weakening the security posture of the different systems and making the organization liable to fines.

P.1 Description of Cardholder Environment

Cardholder data is entered into GVSU's network environment via the following channels: card present, e-commerce, call center, MOTO, fax, and Point of Sales (POS).No cardholder data is stored on GVSU computers, servers or systems. All third party vendors are reviewed for PCI compliance.

P.2 List of Critical Hardware and Software

Stored in #SERVERS and PCI Inventory

P.3 Cardholder Environment Network Diagram

Network Diagrams are located in:

\\office.ads.gvsu.edu\dfs\Tech-Support-Data\PCI\Documentation\Drawings

APPENDIX Q – ACCESS CONTROL MATRIX

Commented [A10]: This is a tool to help organizations develop their own Role Based Access Control model. Different systems will support different types of privileges. This section should go into as much details as necessary to detail the access employees have on their systems. This is just a framework to get started and it should be modified as needed until all the roles are captured.

This appendix documents the Role Based Access Control used at GVSU. The access control is described in 4 sections:

- **Systems and Privileges Available:** This table describes the different systems along with the different access levels which they provide.
- **Roles and Privileges:** This table describes the different roles and their associated privileges to access different systems. The different roles are based on job classification. And the different privileges are based on job functions.
- **Roles and Constrains:** this section describes any constrains that may exist in the model to guarantee proper separation of duties.
- **User and Role Assignments:** This table describes the different users and their assigned role. This table is especially useful for auditing purposes.

Q.1 Systems and Privileges Available

Systems/Objects	Privileges Available
Database (MS SQL / MS Windows 2003)	The GVSU PCI environment does not include any Databases
Web Server (IIS / MS Windows 2003)	The GVSU PCI environment does not include any Web Servers
Authentication and Support Servers	WinServer Admin
Security Devices (Firewall, IPS, FIM)	Network Admin
Log Aggregation System (MS Syslog)	Security Admin
Encryption Keys	The GVSU PCI environment does not store sensitive data
Network Services	Internet; Printer
Testing Environment	The GVSU PCI environment does not require a Test Environment

Q.2 Roles and Privileges

Role	System Access	Granted Privileges
Basic User	Network Services	Internet; Printer
Support	Database	NA
Manager	Database	NA
Developer	Testing Environment	NA
System Administrator	Database	NA
	Web Server	NA
	Security Devices	Network Admin
	AD & Support Servers	WinServer Admin
	Log Aggregation System	Security Admin
	Application System	Group Admin
	Testing Environment	NA

Security Administrator	Log Aggregation System	Security Admin
Key Custodian	Encryption Keys	NA

* Privileges which allow access to Confidential Data. These types of privileges should only be granted to roles which require access to confidential data on a regular basis. See *Information Categories (Section 4.2.2)* for more details about the definition of Confidential Data.

Q.3 Roles and Constraints

- The roles "Developer" and "System Administrator" must be mutually exclusive to guarantee that developers cannot access the production environment without authorization.
- There must be at least 2 "Key Custodian" roles with "Partial Access" to the Encryption Keys to guarantee that more than one person is required to manage the keys.
- The granted privileges marked with a "*" (Access to Confidential Data) must correspond to Roles which have a business need to see this type of data to perform their daily duties.

Q.4 User and Role Assignments

Users/Groups	Roles
Staff Group	Basic User
Support Desk Group	None
Managers Group	None
Development Group	NA
Chief Information Security Officer	None
Jason Kunnen, Dan Barricklow, Bill Fisher	WinServer Admin
Ben Freitag, Jim McPherson, Kyle Neilsen	Network Admin
Greg Vedders, David VanSweden, Luke Demott, Yvonne Bird	Security Admin
Ken Radlick, Mike Grannan, MaryJo Hills, Chris Borema, Todd Michalski, Shannon Hatch, Pete Voss	Group Admin

Important notice: this form and all its associated details must be accessible only by personnel authorized by the Information Technology Department.

APPENDIX R – LIST OF THIRD PARTIES

Refer to \\office.ads.gvsu.edu\dfs\Tech-Support-Data\IT-DIRECTOR-PCI\Inventory\GVSU PCI Application List.xlsx, 3rd Party worksheet

Company Name and Primary Contact	Specific service(s) provided & PCI DSS requirements managed by third party	Elements of Cardholder Data Shared (PAN, expiry date…)	Purpose for Sharing CHD (Third-party storage, transaction processing, etc.)	Status of PCI DSS Compliance (Date of AOC & Version #)	Verified by

20 APPENDIX S – CAPTURE DEVICE INVENTORY LOG

Refer to \\office.ads.gvsu.edu\dfs\Tech-Support-Data\IT-DIRECTOR-PCI\Inventory\GVSU PCI Application List, Elavon terminals and non-Elavon Card present worksheets.

Make/Model	Location	Unique Identifier	Inspection Type	Inspection Frequency

21 APPENDIX T – AUTHORIZED WIRELESS DEVICE INVENTORY LOG

GVSU prohibits wireless device use in the PCI network for processing cardholder data. PCI network environment may be accessed via a GVSU approved laptop meeting security requirements for PCI.

Make/Model	Location	Unique Identifier	Business Justification

INDEX OF PCI REQUIREMENTS

This page is intentionally blank to indicate the end of this document.