Information Security Policies and Procedures

June 2018

Version 9.5

CONFIDENTIAL INFORMATION

This document is the property of Penn Foster; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Penn Foster.

Revision History

Changes	Approving Manager	Date
Initial Publication		
Changes to support an integrated IT Security Policy between The Princeton Review and Penn Foster. Also, made changes to support the MA 201 regulation.		November, 2010
Changes made to correctly depict backup procedures.	Thomas Jones	October 5, 2011
Server build standard additions	Thomas Jones	December 12. 2012
Removed Princeton Review	Thomas Jones	January 22, 2013
Add mobile device policy, correct change management application, and updated VPN tunnel inventory.	Thomas Jones	June 19, 2013
Correction in PII section	Thomas Jones	2/24/2014
Date Correction	Thomas Jones	1/22/2015
Review Corrections	Ray Walton	5/2/2016
Review Corrections to Section 4.5.2, 5.4, and 8.2.10. Changed version to 9.4	Ray Walton, Thomas Jones	3/15/2018

Table of Contents

1 INTRODUCTION AND SCOPE

1.1 Introduction

This document explains Penn Foster's information security requirements for all employees. Penn Foster management has committed to these security policies to protect information utilized by Penn Foster in attaining its business goals. All employees 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 credit cardholder information 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. Concurrent with the announcement, the council released version 1.1 of the PCI standard.

The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit 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).

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, system log server, IDS, PC's performing support functions such as system administration, etc)

1.1 What is MA 201 CMR 17 Compliance?

MA 201 CMR 17 is a data protection regulation that was placed into effect on January 1, 2010. It applies to any business that "own or license personal information, whether paper or electronic records, about a resident of the Commonwealth of Massachusetts". In the case of Penn Foster, this would apply to both customers and employees that are residents of Massachusetts.

MA 201 is similar in nature to PCI Compliance in regards to the security and technical provisions that should be undertake to protect physical assets and computer networks. The biggest difference is in the definition of what types of data must be protected. While PCI is very specific to credit card information, MA 201 opens that up to other information that could be used to steal a person's financial identity. The MA 201 regulation has a specific definition for personal information, or as some refer to it, personally identifiable information. The definition for personally identifiable information can be found in section 4.2.2 Information Categories.

2 POLICY ROLES AND RESPONSIBILITIES

2.1 Policy Applicability

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

2.2 VP of IT and Enterprise Data Services

The VP of IT and Enterprise Data Services holds ultimate authority for decisions pertaining to the information security policies, their content, and any exceptions. The VP of IT and Enterprise Data Services ensures provides executive level visibility and assurance for Penn Foster's information assets.

2.3 Information Security Officer

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

The Information Security Officer or equivalent works closely with the other Penn Foster 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 Security Officer include,

- Make high-level recommendations pertaining to the information security policies and their content. Provide recommendations for exceptions to these policies, on a case-by-case basis, to VP of IT and Enterprise Data Services.
- On an annual basis, 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 third parties, with whom cardholder data is shared, are contractually required to adhere to the PCI DSS requirements and to acknowledge that they are responsible for the security of the cardholder data which they process.
- Complete tasks as required by the *Periodic Operational Security Procedures (Appendix N)*.

2.4 Information Technology Services

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

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

The Information Technology Services is responsible for security planning, education and awareness. Specific responsibilities of the Information Technology Services 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.
- Monitor and analyze security alerts and distribute information to appropriate information security, technical and business unit management personnel.
- Review logs daily. Follow up on any exceptions identified.
- Restrict and monitor access to sensitive areas. Ensure appropriate physical controls are in place where cardholder information is present.
- Complete tasks as required by the *Periodic Operational Security Procedures (Appendix N)*.

2.5 Service Desk

Penn Foster Service Desk are the direct link between information security policies and the network, systems and data. Service Desk responsibilities include,

- Applying Penn Foster information security policies and procedures as applicable to all information assets.
- Administering user account and authentication management.
- Assisting the Information Technology Services with monitoring and controlling all access to Penn Foster data.
- Maintain an up to date network diagram including wireless networks. The diagram must include the date when it was last updated and the name of the employee who performed the update.
- Restrict physical access to publicly accessible network jacks, wireless access points, gateways and hand held devices.
- Completing tasks as required by the *Periodic Operational Security Procedures (Appendix N)*.

2.6 Human Resources 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 Human Resources Department has an important role with regards to Penn Foster information security. The following items are the ongoing responsibility of the Human Resources Department:

- Assist the Information Technology Services with publishing and disseminating Penn Foster information security policies and acceptable use guidance to all relevant system users, including vendors, contractors and business partners.
- Perform background checks on potential employees who will have access to systems, networks, or data, including background, pre-employment, criminal, and reference checks.
- Verify that employees attend awareness training upon hire and at least annually.

- Work with the Information Technology Services on disseminating security awareness information to system users utilizing multiple methods of communicating awareness and educating employees (for example, posters, letters, emails, meetings, etc).
- Work with the Information Technology Services to administer sanctions and disciplinary action relative to violations of Information Security Policy.
- Notify the Information Technology Department when any employee is terminated.

2.7 Users

Each user of Penn Foster 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 Penn Foster 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 Penn Foster in meeting its business goals.
- Maintain awareness of the contents of the information security policies.
- Read and understand the *Penn Foster Security Awareness and Acceptable Use Policy (Appendix A)*.
- Classify confidential and sensitive information that is received unclassified. Limit the distribution of this information accordingly.

3 IT CHANGE CONTROL POLICY

3.1 Policy Applicability

All proposed changes to Penn Foster network devices, systems and application configurations must follow this policy.

3.2 Change Request Submittal

The responsible party that will be implementing the change must complete and submit a *Change Request Form (Appendix C)* to the Information Technology Department.

This form will not be reviewed without at a minimum the following information,

- **Resources Affected by Change (customers)** – If a change could impact the functionality of customers, internal or external, this item must be completed. This documentation must include changes to features, applications and procedures that will be different from the existing system. Included in this documentation are any upgrades that the customer needs to perform to the operating system or other required 3rd party software or hardware.
- **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. This plan may be specific to each change.
- **Management Approval** – All changes must include management approval.

3.3 Change Request Approval

After all planning and documentation is completed, all changes will be reviewed by the Information Technology Change Advisory Committee, which includes IT Management representatives, during the regularly scheduled Change Control meetings. Changes will be approved or denied at that time.

3.4 Change Testing

Prior to introduction into the production network or systems all changes must first be tested on a QA or test environment isolated from the production environment.

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 Penn Foster 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 VP of IT and Enterprise Data Services.

4.2 Data Classification

4.2.1 Introduction

All data stored on Penn Foster 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** – information protected by statutes, regulations, company policy or contractual language. Unauthorized disclosure could seriously and adversely impact the company, stockholders, business partners, employees, and/or its customers. Examples of confidential information include passwords, encryption keys, financial statements, strategic corporate documents, trade secrets, customer lists, etc.
- **Personally Identifiable Information (PII) –** PII data pertains to an information about an individual, whether a customer or an employee. It is defined as an individual's First Name and Last name, or First Initial and Last Name used in conjunction with any of the following information:
  - National or State Issued Identification Numbers including:
    - Social Security Number or Individual Taxpayer Identification Number
    - Passport Number
    - Driver's License Number
    - State Identification Number
  - Birth Place
  - Financial Account Number
  - Credit Card Number
  - Digital Identity (supporting authentication such as, PIN, CVV2, password, etc.)
  - Biometric Data (fingerprints, handwriting, etc.).
- **Sensitive** – information that must be protected due to proprietary, ethical, or privacy considerations (although not falling into the category of PII). Unauthorized disclosure could adversely impact the company, its stockholders, its business partners, employees and/or its customers. Examples of sensitive information include sales plans, internal market research, audit reports, internal directories, software source code, 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 Penn Foster Public Relations Department.

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 Services 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 Penn Foster 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 *Information Technology Access Request Form (Appendix G)* by completing and submitting 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. Requests for new employees are sent to Human Resources via Personnel Action Form. The Human Resources Department will perform a formal background check for all new employees.

    b. If the request is for an existing employee, the form must be sent to the Information Technology Services.

2. The Information Technology Services 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 Services. If the access requested requires privileges above the user's role the Information Technology Services will engage additional system owners or management to collect approvals.

3. Once the Information Technology Services approves the request, a Service Desk will execute the request.

4. The Service Desk will create the user account(s) requested.

5. The Service Desk will forward the completed request form to the requesting manager.

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 Human Resources Department or the employee's manager.

4.4 Physical Security

Hard copy materials and electronic media containing confidential or personally identifiable information (PII) must be protected by appropriate physical access controls.

- Cameras must be used to monitor sensitive areas. The data collected must be stored for at least 3 months unless otherwise restricted by law.
- Appropriate facility controls must be used to limit and monitor physical access to systems that store confidential or personally identifiable information.
- Visitor logs and physical audit trails of access to these systems must be collected and kept at least 3 months unless otherwise restricted by law.
- Physical access must be restricted to publicly accessible network jacks, wireless access points and handheld devices.

4.5 User Authentication

4.5.1 Users

Each user's access privileges shall be authorized according to business need. User access authority to computer resources shall be provided only when necessary to perform tasks related to Penn Foster's business.

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 never permitted for user-level access.

Every user must use a unique user account and a personal secret password for access to Penn Foster information systems and networks. Systems and applications must authenticate using a password or token entry. Passwords should be kept secret by every user. They should not be written down or shared with anyone including family, friends, co-workers, supervisors or even the IT staff.

All users must acknowledge understanding of Penn Foster Information Security Policies prior to being allowed to access Penn Foster information systems and networks.

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).
- Penn Foster employee user ID's will be unique.
- Non-employee user ID's will consist of the prefaced by cntr followed by underscore and followed by the first initial and last name of the contractor. Description should include contractor company name.
- Authenticate every user ID, system account and application account 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 three invalid logon attempts.
- Require that once a user account is locked out it remains locked for thirty (30) minutes or until the Service Desk resets the account.
- Require system/session idle time out of 15 minutes.
- Require passwords to be reset at least every 90 days. Note: Job/Service user IDs may be exempt from this requirement with management approval. Administrative user IDs (e.g. root, oracle, Administrator) 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).
- Disable inactive users at least every 90 days.

4.6 Account and Access Management

4.6.1 Information Technology Services Responsibilities

The Information Technology Services 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 Services, in conjunction with business unit management, will define the different roles and the minimum access level associated to each role.

A member of the Information Technology Services must review the Access Authorization Form to assure proper separation of duties.

The Information Technology Services 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.

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

4.6.2 Service Desk Responsibilities

The Service Desk 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)*.
- User IDs shall be disabled after ninety (90) days of inactivity. After an additional thirty (30) days, disabled user IDs must be purged. These requirements may not apply to certain specialized accounts. In those instances, the Service Desk must provide a written waiver to the Information Technology Services and document the compensating controls around access to the accounts.

- All computer resources capable of displaying a custom sign-on or similar message must display the following message as part of the login process:

```
Please be aware you are entering a restricted system. All data and
information herein may be considered as confidential and proprietary to
Penn Foster Education Inc. Please ensure you have the proper authorization
before proceeding. All activity on this system is subject to monitoring.
Where such monitoring reveals unauthorized use and/or inappropriate access
or use, Penn Foster Education Inc. shall invoke all applicable rights to
investigate discipline and/or prosecute violators. By clicking OK you agree
to abide by all policies set forth by Penn Foster.
```

- Passwords set by Service Desk must be changed by the user immediately upon the users' next login. Service Desk must set initial passwords that are unique and compliant with the password rules.
- Service Desk must validate the identity of users before performing a password reset. The approved means for validating identity at Penn Foster is by doing it in person with a valid employee ID, or remotely by providing uniquely identifying pieces of information. Examples could include: employee ID, full name, manager's name, and home phone number.
- Contractor accounts must have Information Technology Services approval and must automatically expire at the end of the contract date. Extensions must be requested through the Information Technology Services. Service Desks 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 8.3)* must be followed to connect and disconnect all external entities.
- Ensure that all systems and especially access to any databases containing cardholder information is authenticated (e.g., users, applications, administrators, etc.). Direct SQL queries to the database should be limited to database administrators.
- Service Desk 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 Infrastructure Team.

5 DATA RETENTION AND DISPOSAL POLICY

5.1 Policy Applicability

All data deemed confidential or personally identifiable information (PII) by the Information Technology Services which is stored on Penn Foster networks and systems must follow this policy. Exemptions from this policy will be permitted only if approved in advance and in writing by the VP of IT and Enterprise Data Services.

5.2 Retention Requirements

All confidential and personally identifiable information (PII), 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 VP of IT and Enterprise Data Services.

As a special case, cardholder data used for single transactions may be kept for up to 120 days. This applies for cardholder data retained in any kind of format including digital and paper. Check for accuracy.

Cardholder data utilized for recurring transactions may be retained for the lifetime of the customer's account with Penn Foster. 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 "authorization data", including track, CVV2, and PIN information, will be retained only until completion of the authorization of a transaction. Storage of cardholder authorization data post-authorization is forbidden.

All system and network audit logs must be retained for one year with 90 days available for online viewing.

5.3 Disposal Requirements

All confidential data or personally identifiable information (PII) in electronic format, when no longer needed for legal, regulatory or business requirements must be removed from Penn Foster 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 data or personally identifiable information (PII) in hardcopy format, 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

A programmatic (automatic) process will be executed on cardholder information systems nightly to remove all confidential data or personally identifiable information (PII) that exceeds business retention 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 Services.

Media containing confidential data or personally identifiable information (PII) that should no longer be retained must be disposed of in a secure and safe manner as noted below:

- Hard disks: Degauss and destroy platter.
- Tape media: degauss, shred, incinerate, pulverize or melt.
- USB "thumb" drives, smart cards, and digital media: incinerate, pulverize or melt.
- Optical disks (CDs and DVDs): destroy optical surface, incinerate, pulverize, shred or melt.

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

Outsourced destruction of media containing confidential data or personally identifiable information (PII) must use a bonded Disposal Vendor that provides a "Certificate of Destruction".

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 VP of IT and Enterprise Data Services.

6.2 Storage

6.2.1 Physical Security

Hard copy materials and electronic media containing confidential data or personally identifiable information (PII) must be protected by appropriate physical access controls.

- Cameras must be used to monitor sensitive areas. The data collected must be stored for at least 3 months.
- Appropriate facility controls must be used to limit and monitor physical access to systems that store confidential data or personally identifiable information (PII).
- Visitor logs and physical audit trails of access to these systems must be collected and kept at least 3 months unless otherwise restricted by law.

6.2.2 Hardcopy Media

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

- At no time are printed reports containing confidential data or personally identifiable information (PII) to be removed from any Penn Foster secure office environment.
- Printed reports containing personally identifiable information (PII) are to be physically retained, stored or archived only within secure Penn Foster office environments, and only for the minimum time deemed necessary for their use.
- All hardcopy material containing confidential data or personally identifiable information (PII) should be clearly labeled as such.
- All personally identifiable information (PII) 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 Services.
- Personally identifiable information (PII) hardcopy material is never to be stored in unlocked or insecure containers or open workspaces.
- When no longer needed, confidential data or personally identifiable information (PII) in hardcopy format should be shredded according to Penn Foster Shredding Policy.

6.2.3 Electronic Media

Electronic media containing confidential data or personally identifiable information (e.g., CD, DVD, hard disk, tape, etc.) is subject to the following storage guidelines:

- Personally identifiable information (PII) must never be copied onto removable media without authorization from the Information Technology Services.

- At no time is electronic media containing personally identifiable information (PII) to be removed from any Penn Foster secure office environment with the exception of computer system backups.
- Electronic media containing personally identifiable information (PII) are to be physically retained, stored or archived only within secure Penn Foster office environments, and only for the minimum time deemed necessary for their use.
- All electronic media containing confidential data or personally identifiable information (PII) should be clearly labeled as such.
- All removable electronic media containing personally identifiable information (PII) must be stored securely.
- All media containing confidential data or personally identifiable information (PII) must be sent or delivered by a secured courier or other delivery methods that can be accurately tracked and that have been approved by the Information Technology Services.
- Personally Identifiable Information (PII) should never be placed on a wireless smartphone or mobile computer.

6.3 Inventory

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

6.4 Destruction

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.

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

7 FIREWALL AND ROUTER SECURITY ADMINISTRATION POLICY

7.1 Policy Applicability

All firewalls and routers on Penn Foster 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 VP of IT and Enterprise Data Services.

7.2 Device Management Responsibilities

Management of all Penn Foster firewalls and routers shall be the responsibility of the Information Technology Services. The following subsections detail the responsibilities for these groups.

7.2.1 Infrastructure Team

- Assure that changes to firewall hardware or software or security rules are approved by the Information Technology Services and follow all change control policies and procedures.
- Document all firewall security rule changes using work order process.
- Following every change, review and update network diagrams to assure they accurately describe all connections to personally identifiable information (PII) 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 Information Technology Services immediately upon discovery.
- Coordinate an appropriate response with the Information Technology Services to mitigate security events.
- Ensure that router configuration files are secured and synchronized properly.
- 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.

7.2.2 Information Technology Services

- Assure that security rules applied to the firewalls are sufficient to protect Penn Foster networks and corporate assets from external attacks and unauthorized access.
- Assure that security rules applied to the firewalls are sufficient to prevent internal security events from leaving Penn Foster 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 are properly documented
- Ensure risky protocols have undergone a risk assessment, have a current documented business need, and are secured as per documented security standard. For the PCI environment, compensating controls will be required for risky protocols such as Telnet and FTP.

- Actively monitor firewall security events to identify internal or external security incidents.
- Conduct quarterly review of all firewall and router rule sets.
- Coordinate an appropriate response with the Service Desk to mitigate security events.

7.3 Allowed Services

Every connectivity path and service that is not specifically permitted by this policy, with supporting documents issued by the Information Technology Services, must be blocked by Penn Foster firewalls. The list of currently approved paths and services, with justifications can be obtained by our Work Order system.

7.4 Allowed Network Connection Paths and Configuration Requirements

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 ports necessary for Penn Foster's business requirements. Perimeter routers should not be configured with a route to internal address space with the exception of the DMZ.

Internal IP addresses must be hidden utilizing Network Address Translation (NAT) or Port Address Translation (PAT).

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

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

Outbound traffic from internal production systems must only be allowed to the Penn Foster DMZ network. Additionally, this traffic should be restricted to only required protocols and services.

Databases must be located on an internal network which is segmented from the Penn Foster DMZ network. Inbound connections to internal production payment systems, and originating from Penn Foster wireless networks, are not permitted.

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 cardholder 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 segmenting all requirements for firewalls apply (e.g. deny all but business necessary traffic, change control, etc).

7.5 Configuration Review

Every six months, the Information Technology Services must thoroughly review each firewall rule set and record results of the review. The review must include the removal, when merited, of unused or unnecessary access paths. All proposed changes identified as a result of this review must go through the current change control process prior to implementation.

7.6 Personal Firewalls

All mobile and/or employee-owned computers (e.g., laptops used by employees) that are used to access Penn Foster network must have personal firewall software installed and activated. All such software must have a non-user alterable configuration created by the Information Technology Services.

8 SYSTEM CONFIGURATION POLICY

8.1 Policy Applicability

All servers and network devices on Penn Foster 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 VP of IT and Enterprise Data Services.

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).

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 Penn Foster published configuration standards. Deviations require written approval by the Information Technology Services and must be noted on the *System Configuration Record (Appendix H)* for the system.

8.2.3 System Configuration Records

A *System Configuration Record* 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. This document is found on a tab of the server requisition form.

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 systems purpose.
5. Update all application software per vendor recommendations.
6. Configure application parameters according to the *System Configuration Standards (Appendix B)*.
7. Enable logging per *Logging Controls (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.

8.2.5 File Integrity Monitor (FIM) Software

For systems storing or processing personally identifiable information (PII) deploy file integrity monitoring (FIM) software to alert personnel to unauthorized modification of critical system or content files. Configure FIM 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 cardholder environment via the Internet must have the following software installed:

- Personal Firewall software which users should not be able to disable.
- VPN Client software capable of supporting the company's 2-factor authentication solution.

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 Network Time Protocol (NTP)

All Penn Foster production systems must be configured to use one of the approved NTP servers to maintain time synchronization with other systems in the environment.

At least 2 internal Penn Foster 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 available version of the software.

8.2.9 Credit Card Information Processing Application

All Penn Foster applications dealing with the processing or retrieval of cardholder information, must, where there is not a business need to display full PAN, mask displayed primary account numbers (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 Services during the Requirements Phase as described in the *Software Development Policy (*Section *13)*. In all cases the application must limit the display of the full PAN to the fewest number of users possible.

8.2.10 Credit Card Storage Applications

All Penn Foster applications dealing with the storage of cardholder data must be configured in a manner which does not retain sensitive cardholder data such as full track data, card-validation codes, card not present values, pins or pin blocks. Storage devices on a network must be on an internal network segregated from the DMZ. 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.
- Truncation.

- Index tokens and pads (pads must be securely stored).
- Strong cryptography with associated key management processes and procedures.

In particular, 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. If cardholder data is ever received from wireless networks it must be rendered unreadable wherever stored.

8.3 8.3 Vulnerability Identification and System Updates

8.3.1 Vulnerability Identification

Members of the Information Technology Services must be informed of information security issues and vulnerabilities applicable to Penn Foster computing systems. When security issues are identified, the Information Technology Services is responsible for notifying appropriate personnel, including Service Desks.

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 Penn Foster specific software packages and systems:

- CERT
- NT BUGTRAQ
- SANS

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

8.3.2 Vulnerability Testing

The Information Technology Services 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). This process includes identifying any unauthorized wireless devices on the network.

Additional external vulnerability scans must be performed by a scan vendor qualified by the payment card industry at least quarterly. The results of each scan must satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities).

Penetration tests at both the application and network layer must be performed annually or after any significant change in the network. Penn Foster will utilize a security company who is qualified to perform internal as well as external penetration testing.

Networks and systems that fall under payment card system scope must also be monitored by an intrusion detection/prevention system that alerts personnel of potential compromises.

All potential vulnerabilities identified through vulnerability scans and penetration tests will be communicated to appropriate personnel within Penn Foster for assessment and remediation. All high-level vulnerabilities must be corrected utilizing the *Change Control Policy (Section 3)*. Follow up scans must be performed to confirm compliance with Penn Foster security standards.

The VP of IT and Enterprise Data Services must coordinate an annual formal risk assessment process that identifies any existing or new threats and vulnerabilities to ensure Penn Foster assets are adequately protected.

8.3.3 Security Patch Deployment

All security patches, hot-fixes and service packs identified by the Information Technology Services or the Service Desk, must be installed on applicable systems within thirty (30) days of vendor release. As with any change to the environment, the change management process must be followed.

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 Penn Foster network environment. In particular, the following must be followed:

- Technologies such as SSH, VPN or SSL/TLS must be used for all remote administration.
- All remote access to Penn Foster 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 Service Desk 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.

9 ANTI-VIRUS POLICY

9.1 Policy Applicability

All system commonly affected by viruses such as servers, workstations and laptops on Penn Foster 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 VP of IT and Enterprise Data Services.

9.2 Software Configuration

All applicable systems must be configured with Information Technology Services approved anti-virus/anti-spyware/anti-adware software. 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.

9.3 Signature Updates

All systems with anti-virus software must be configured to update virus signatures or equivalent. Scan engines, if applicable, should scan at least on a weekly basis for servers and PCs.

9.4 Software Logging

Anti-virus software must alert the Information Technology Services in real-time to the detection of a virus.

The Information Technology Services 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).*

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 Security Officer.

10.2 Procedures

All systems are backed up to tape, disk, or cloud based backup systems. The jobs are monitored daily by the Operations staff by email and daily reports. Any corrective actions would be executed by the Operations staff. If jobs are run over their allotted time the Operations staff lets the job complete.

Tape based Full backups are completed weekly on Sundays and Incremental are completed Monday through Saturday. Retention is three months of Full backups and two weeks of incremental backups. On Tuesday the tapes are vaulted offsite to a secure third party location. Encryption is handled by the source application.

Disk based backup onto storage servers synchronization points are completed once daily. The retention period is for two weeks. This is the equivalent of running and retaining daily Full tape backups. After the completion of the daily jobs are replicated to another storage server. Encryption when necessary is handled by the backup software.

Cloud based Full backups, to Barracuda are completed daily. The retention period is for two weeks. This is the equivalent of running and retaining daily Full tape backups. The data is encrypted while in transit and at rest at the third party location.

10.3 Location

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

10.4 Transport

Offline storage media utilized for archival or back-up purposes must be handled and retained in a secured environment such that only Penn Foster 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 Services.

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 data or Personally Identifiable Information (PII) must be classified and identifiable as such prior to transfer as detailed in the *Data Classification and Control Policy (Section 4).*

Backup media which contains data constituting Personally Identifiable Information must be encrypted prior to transport.

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 Penn Foster 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 Penn Foster must include these guidelines. Exemptions from this policy will be permitted only if approved in advance and in writing by the VP of IT and Enterprise Data Services.

11.2 Encryption Key Management

Keys must be generated, accessed, distributed and stored in a controlled and secured manner.

11.2.1 Key Access

Keys used to encrypt and decrypt cardholder data 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 VP of IT and Enterprise Data Services 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 Information Technology Services.

11.2.2 Split Knowledge and Dual Control

When an encryption key is known in clear text a minimum of two custodians, authorized by the Information Technology Services, are required to collaborate to perform any key action (such as key generation or loading the key). Additionally, no single custodian may know or have access to all pieces of a data encryption key.

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,

- Triple-DES – 128 bits
- AES – 256 bits
- RSA – 2048 bits
- Industry recommendations/best practices for other encryption methodologies

Generating encryption keys must be accomplished by a minimum of two custodians authorized by the Information Technology Services. Each custodian will generate one clear text piece 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.

11.2.4 Key Distribution

Only custodians authorized by the Information Technology Services are allowed to retrieve key components from secure storage or distribute keys. Custodians must document all such actions in the *Encryption Key Management Log (Appendix J)*. The encryption keys must be placed in secure packaging prior to being returned to storage.

11.2.5 Key Storage

All data encryption keys must be stored encrypted and in a secure location. Key-encrypting keys must be stored separately from data-encrypting keys within all applicable programs.

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

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 encryption 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 Rotation: Keys must be changed at least every year.
- Suspicious Activity: This change is driven by any activity related to the key process which raises concern regarding the security of the existing key.
- Resource Change: Keys must be changed if a resource with knowledge of the keys 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.

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).*

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. Some examples of strong encryption that is acceptable are,

- Transport Layer Security (TLS1.2)
- Internet Protocol Security (IPSEC)

11.3.1 Email Transmission of Confidential Information

Confidential and sensitive information is never to be sent unencrypted through email without first discussing the need to the Information Technology Services. Employees, with a valid business justification for emailing confidential or Personally Identifiable Information (PII), must be provided with an email encryption solution by the Information Technology Services.

11.3.2 Encryption of Wireless Networks

All wireless networks in use at Penn Foster facilities must be protected through secure data encryption such as Wi-Fi Protected Access (WPA2), IPSEC VPN, or TLS. Under no circumstances should the encryption strength be configured to be less than 128 bits.

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 (for example, not using local or Active Directory accounts).
- Make sure that the decryption keys are not associated with user accounts.
- Verify that decryption keys are not stored on the local system (for example, store keys on USB thumb drives or CD-ROM that can be secured and retrieved only when needed).
- Ensure that Personally Identifiable Information (PII) data, including cardholder data, on removable media is encrypted wherever stored (disk encryption often cannot encrypt removable media).

12 SOFTWARE DEVELOPMENT POLICY

12.1 Policy Applicability

All development efforts of software designed to run on Penn Foster 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 VP of IT and Enterprise Data Services.

12.2 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 Penn Foster network, access controls must be in place to enforce the separation.

Production data (real credit card numbers) will not be used for testing and development purposes without being sanitized. Test personnel should make every effort to use mock data only for testing on non-production systems and software.

All test data, custom application accounts, usernames and passwords must be removed at the conclusion of testing, and in all cases before software becomes active.

All code promotion to the production environment will be accomplished by the Service Desks. Under no circumstances will the 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 Services Responsibilities (Section 4.6.1).*

12.3 Secure Software Development Procedures

12.3.1 Development Life-Cycle

Internal and 3rd party development of proprietary software must utilize industry recognized best practices for software development. 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 Penn Foster development process are as follows,

1 **Concept** - Projects are envisioned and prioritized
2 **Inception** - Team members are identified, funding is put in place, and initial environments and requirements are discussed
3 **Iteration/Construction** - The development team works to deliver working software based on iteration requirements and feedback
4 **Release** - QA (Quality Assurance) testing, internal and external training, documentation development, and final release of the iteration into production
5 **Production** - Ongoing support of the software
6 **Retirement** - End-of-life activities, including customer notification and migration

12.3.2 Web-based Applications

In addition to all the security measures that take place throughout the application development life-cycle, special care should be given to Penn Foster applications that are web-based.

All Penn Foster developers will receive training on secure coding practices. All development must be done taking the Open Web Application Security Project OWASP guidelines into account, located at http://www.owasp.org. Specifically, the following vulnerabilities must be considered during the Code Review and Testing phases as per PCI DSS version 3.1:

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 8.2.2).*

12.3.3 Credit Card Informational and Processing Applications

All Penn Foster proprietary or custom applications that process card holder information should utilize tokenization for Payment Card Number processing. In the case where tokenization is not possible it must be documented and follow the following requirements for retrieval of the PAN:

Processing or retrieval of cardholder information must be configured in a manner which masks or truncates the displayed credit card number. If cardholder information is to be masked only the first 6 and last 4 digits may remain displayed. 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 Services.

13 INCIDENT RESPONSE PLAN AND PROCEDURES

13.1 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 VP of IT and Enterprise Data Services.

A separate procedure document has been established to cover any type of security breach involving Personally Identifiable Information (PII). Please see the procedure entitled Incident Response Plan – Breach of Personal Information if the incident involves Personally Identifiable Information (PII).

13.2 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, abnormal errors in system log files or on terminals)
- Security event notifications (e.g., file integrity alerts, intrusion detection alarms, and physical security alarms)

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 14.3 Incident Reporting, unless they are assigned other activities within the incident response plan.

13.3 Reporting and Incident Declaration Procedures

The Information Technology Services should be notified immediately of any suspected or real security incidents involving Penn Foster computing assets, particularly any critical system. If it is unclear as to whether a situation should be considered a security incident, the Information Technology Services 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 Information Technology Services personnel or under the oversight of Information Technology Services personnel, to assure the integrity of the incident investigation and recovery process. When faced with a potential situation you should do the following,

- If the incident involves a compromised computer system.
  - Do not alter the state of the computer system.
    - The computer system should remain on and all currently running computer programs left as is. 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.

- Report the security incident.
  - Contact the Information Technology Services to report any suspected or actual incidents.
  - No one should communicate with anyone outside of their supervisor(s) or the Information Technology Services about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Information Technology Services.
  - Document any information you know while waiting for the Information Technology Services 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.

13.4 Incident Severity Classification

The Information Technology Services 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 Services 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 Personally Identifiable Information (PII) or originating from unauthorized internal systems is classified as a Level 2.

13.5 Incident Response

13.5.1 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 Services once an incident has been identified and classified.

13.5.1.1 Level 1

Contain and Monitor

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

13.5.1.2 Level 2

Contain, Monitor and Warn

1. Collect and protect information associated with the intrusion.
2. Utilize approved technology controls to temporarily or permanently block the intruder's access.
3. Research the origin of the connection.
4. Contact the Internet Service Provider (ISP) and ask for more information regarding the attempt and intruder.
5. 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.
6. 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 Human Resources Department to address the Acceptable Use violation appropriately.

13.5.1.3 Level 3

Contain, Eradicate, Recover and perform Root Cause Analysis

1. If the incident involved credit card systems the Acquirer and applicable card associations must be notified. See the *Credit Card Compromise – Special Response (Section 14.5.2)* for more details.
2. 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 userID, terminating the user's session/change password etc.
3. Collect and protect information associated with the intrusion via offline methods. In the event that forensic investigation is required the Information Technology Services will work with legal and management to identify appropriate forensic specialists.
4. Notify management of the situation and maintain notification of progress at each following step.
5. Eliminate the intruder's means of access and any related vulnerabilities.
6. Research the origin of the connection.
7. Contact the ISP and ask for more information regarding attempt and intruder, reminding them of their responsibility to assist in this regard.

8. Research potential risks related to or damage caused by intrusion method used.

13.5.2 Personally Identifiable Information – Special Response

For any incidents involving potential compromises of Personally Identifiably Information (PII), the Information Technology Services will use the procedures documented in the Incident Response Plan – Personally Identifiable Information.

13.5.3 Root Cause Analysis and Lessons Learned

Not more than one week following the incident, members of the Information Technology Services 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)*.

13.6 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 Services. Once complete, a follow-up session, as detailed above in section 14.5.3, will be held.

All Penn Foster 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.

13.7 Automated Security System Notifications

All automated intrusion detection systems within Penn Foster environment, including intrusion detection sensors and file integrity checking systems, will be configured to automatically notify the Information Technology Services of any potential compromises or attacks.

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

13.8 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 Information Technology Department must guarantee that critical business functions continue with minimal impact until all systems are restored to normal operations.

14 EMPLOYEE IDENTIFICATION POLICY

14.1 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 VP of IT and Enterprise Data Services.

14.2 Employee Requirements

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

14.3 Facilities

The Information Technology Services must locate the badge creation system in a physically secure environment.

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 three (3) months.

14.4 Badge Assignment Procedure

14.4.1 New Badges

The Human Resources Department will create and manage all employee badges. Human Resources will issue the badge to the new employee, with only approved access levels.

14.4.2 Visitor Badges

A visitor 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).

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

14.4.3 Changing Access

All requests for a change in access level must be made directly to the Jira system and handled by the Facilities Manager. If the access request is approved, the Facilities Manager will make the modification.

14.4.4 Revoking Badges

Upon being notified of an employee termination Facilities/HR will immediately disable all badge accesses for the terminated employee.

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

15 LOGGING CONTROLS POLICY

15.1 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 VP of IT and Enterprise Data Services.

15.2 Events Logged

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

- All user access to Personally Identifiable Information (PII) data.
- All administrative actions utilizing user IDs with significant privileges above a general user (e.g. root, user IDs with Administrator group privilege, oracle, etc).
- Access to audit log files.
- Any user or administrator authentication attempts (both valid and invalid).
- Identification and authentication mechanism used.
- Creation or deletion of system-level objects (for example, executables, libraries, configuration files, drivers, etc).
- Initialization of audit log files.

15.3 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.
- Originating location of the event.
- The name of the affected data, system component or resource.

15.4 Log Security

Where ever practical, all event logs should be collected in a centralized location or media that is difficult to alter and protected from unauthorized access. 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 that alerts the Information Technology Services upon unauthorized access. Wireless logs must be copied onto a log server on the internal LAN Log Monitoring The system event logs must be monitored by the Network and Systems Administrators in the Information Technology Department every day. The Network and Systems Administrators must develop procedures and automated routines to facilitate the efficient and effective audit of system logs to both prevent and discover unauthorized usage of systems and data.

APPENDIX A – SECURITY AWARENESS AND ACCEPTABLE USE POLICY

Penn Foster Security Awareness

And Acceptable Use Policy

Overview

The intentions for publishing a security awareness and acceptable use policy are not to impose restrictions that are contrary to the established culture of openness, trust and integrity. Penn Foster is committed to protecting all employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Penn Foster. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Penn Foster employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Penn Foster. These rules are in place to protect the employees and Penn Foster. Inappropriate use exposes Penn Foster to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees, contractors, consultants, temporary employees, and all other workers at Penn Foster, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Penn Foster.

Employees, contractors, temporary employees of Penn Foster who are provided access to the company's computer network must review and sign this policy annually.

Policy

General Use and Ownership

1. While the Information technology Services team desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Penn Foster. Because of the need to protect the company's network and computer assets, management cannot guarantee the confidentiality of employee's personal information stored on any network device belonging to Penn Foster.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. IT recommends that any information that users consider sensitive or vulnerable be encrypted.
4. For security and network maintenance purposes, authorized individuals within Penn Foster may monitor equipment, systems and network traffic at any time.
5. Penn Foster reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. Information can be categorized as documented below:

a. **Confidential** – information protected by statutes, regulations, company policy or contractual language. Unauthorized disclosure could seriously and adversely impact the company, stockholders, business partners, employees, and/or its customers. Examples of confidential information include passwords, encryption keys, financial statements, strategic corporate documents, trade secrets, customer lists, etc.

b. **Personally Identifiable Information (PII) –** PII data pertains to an information about an individual, whether a customer or an employee. It is defined as an individual's First Name and Last name, or First Initial and Last Name used in conjunction with any of the following information:

   i. National or State Issued Identification Numbers including:
   ii. Social Security Number or Individual Taxpayer Identification Number
   iii. Passport Number
   iv. Driver's License Number
   v. State Identification Number
   vi. Birth Place
   vii. Financial Account Number
   viii. Credit Card Number
   ix. Digital Identity (supporting authentication such as, PIN, CVV2, password, etc.)
   x. Biometric Data (fingerprints, handwriting, etc.).

c. **Sensitive** – information that must be protected due to proprietary, ethical, or privacy considerations (although not falling into the category of PII). Unauthorized disclosure could adversely impact the company, its stockholders, its business partners, employees and/or its customers. Examples of sensitive information include sales plans, internal market research, audit reports, internal directories, software source code, etc.

d. **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 Penn Foster Public Relations Department.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Passwords should never be written down and they should never be told to anyone including friends, family, co-workers, supervisors and the IT staff. System and user level passwords should be changed every 90 days.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less.
4. Employees should secure their workstations by logging off or locking (control-alt-delete for Windows users) when the host will be unattended.
5. Use encryption of information in compliance with Information Technologies' Security Policies.
6. Personally Identifiable Information (including SSNs, credit cards and bank account numbers) should never be stored on your PC, laptop or any removable media (CDs, flash drives, etc.). Further, hardcopy reports containing any of this information should never leave a secure office location. Personally Identifiable Information should never be sent via email or file transfer if not properly encrypted. Employees with a need to send PII data via email or any other type of file transfer should contact the IT department for assistance in setting up the proper safeguards.

7. Because information contained on portable computers is especially vulnerable, special care should be exercised to minimize the risk of loss or theft. Protect laptops in accordance with the corporate security standards, including personal firewalls.
8. Postings by employees from a Penn Foster email address to newsgroups or blogs are prohibited unless the posting is approved by Penn Foster management team in the course of business duties.
9. Only computers owned by the company should be used by an employee to connect to the Penn Foster Internet/Intranet/Extranet. The IT Department configures these computers to meet the company's security policy.
10. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Penn Foster authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Penn Foster-owned computer resources.

The list below is by no means exhaustive, but is an attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Penn Foster.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Penn Foster or the end user does not have an active license is strictly prohibited. The use of any recording device such as, but not limited to, digital cameras, video cameras, and cell phone cameras, within the premises of all Penn Foster properties is prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Penn Foster computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Penn Foster account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient (especially involving confidential or PII data) or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For

purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to IT is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's computer, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any computer, network device or user account.
13. Interfering with or denying service to any user other than the employee's computer (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Penn Foster employees or customers to parties outside Penn Foster.
16. Attaching personally owned computers to the company's computer network. Only the Information Technology department may place switches, routers, or wireless access points on the company network.
17. Manipulating a computer's configuration to allow any employee other than those in the IT Department to possess "local administrator" rights. Doing so makes the end user vulnerable to computer viruses and hacking attempts.
18. Moving or unplugging any computer equipment, other than laptop computers, unless instructed to do so by the Information Technology department.
19. Purchase of any computer hardware (including but not limited to switches, routers, wireless access points, computers, laptops, printers and scanners) and/or software by an employee that is not an authorized IT Department purchaser. End users may not purchase any of these items and expense them.
20. Installation of any software on a company owned computer without being supervised by a staff member of the Information Technology Department.
21. Keeping outdated computer equipment in service even though the IT Department has provided replacement equipment and asked for the equipment to be returned. Older equipment may not provide the most up-to-date security capabilities. Continued use of older equipment puts the entire company network at an unacceptable risk.
22. Circumvention of the company's procedures and/or software intended to block end user's access to inappropriate or dangerous websites. The company employs a software tool that provides website filtering to facilitate blocking employees from internet websites deemed to be inappropriate or dangerous from a security standpoint. There are thought to be over 100 million websites on the internet, so categorizing them all is not an exact science. If an end user believes that our software has inaccurately categorized a website, they may contact the company's Director of Technical Operatios..
23. Allowing non-employees (excluding appropriate vendors, consultants, contractors or temporary employees) to connect equipment to the company network.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Using the company computer or telephony assets to perpetrate any form of harassment via email, telephone or paging, whether through the content of language, frequency, or size of messages.
3. Unauthorized use, or forging (spoofing), of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Penn Foster's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Penn Foster or connected via Penn Foster's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

APPENDIX B – SYSTEM CONFIGURATION STANDARDS

Applicability

This appendix includes hardening and installation procedures for all off-the-shelf operating systems and applications used at Penn Foster. All installations of these operating systems and applications must adhere to these requirements.

The latest system configuration standard is available on Penn Foster Intranet.

APPENDIX C – CHANGE REQUEST FORM

Penn Foster Change Request Form

Penn Foster Change Request form is available in electronic form via Jira. The link to Jira can be found below.

Jira

APPENDIX D – MEDIA INVENTORY LOG

Penn Foster Media Inventory Log

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
				□ Yes □ No
				□ Yes □ No

APPENDIX E – BACKUP MEDIA TRANSFER LOG

Penn Foster Media Transfer Log

Date	Container #	Courier Signature	Management Signature

APPENDIX F – PERMITTED NETWORK SERVICES AND PROTOCOLS

The current list of permitted network protocols and services are available within the Firewall management station and the firewall rule request documents in our Trackit work order system.

Trackit

APPENDIX G – AUTHORIZATION REQUEST FORM

Penn Foster Authorization Request Form

Penn Foster IT Access Control system (ITAC) is available via the link below.

ITAC

APPENDIX H – SYSTEM CONFIGURATION RECORD

Penn Foster System Configuration Record

System configuration records can be found on the Penn Foster Intranet via the link below:

Server Build documents

APPENDIX I – ENCRYPTION KEY CUSTODIANSHIP FORM

Penn Foster Encryption Key Custodianship Form

Encryption key custodians are those person(s) delegated the responsibility of managing, handling and protecting access to Penn Foster encryption keys. Custodians are responsible for the safety and integrity of keys in their custody. The custodian has responsibility to:

- Implement all encryption key controls as specified by the Information Technology Services 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.

_____ _____

Key Custodian Signature Date

_____

Printed Name

APPENDIX J – ENCRYPTION KEY MANAGEMENT LOG

Penn Foster Encryption Key Management Log

Date	Time	Key	Custodian and Witness	Reason

APPENDIX M – VISITOR LOG

Penn Foster Data Center Visitor Log

Date	Time In	Name	Company	Authorized Employee	Time Out

APPENDIX N – PERIODIC OPERATIONAL SECURITY PROCEDURES

Penn Foster Periodic Operational Security Procedures

Task	Daily	Monthly	Quarterly	Bi-Annual	Annually	Target Window
Security Policy						
Enterprise Risk Analysis					X	Q3
Policy/standards review					X	Q3
Security awareness orientation					X	Q3
Organizational Security						
Review security policy exceptions compliance				X		Q3
Asset Classification and Control						
Review system access controls				X		Q2 and Q3
Review access request approvals & audit trail				X		Q2 and Q3
Audit disposal of data and media			X			Week-2
Personnel Security						
Audit terminated employee samples for system, network, application access			X			Week-4
Incident response team meeting			X			Week-1
Physical and Environmental Security						
Visit offsite storage facility and perform media inventory					X	Q3
Review compliance of data center access & visitor logs					X	Q3
System Security						
File Integrity Scan	X					1 a.m.
Review intrusion detection (IDS/IPS) logs	X					8 a.m.
Review all other security and event logs	X					8 a.m.
External vulnerability scan			X			Week-3
Internal vulnerability scan			X			Week-3
Use a Wireless Analyzer to detect unauthorized wireless devices in use			X			Week-3
Firewall rule set review				X		Q1/Q3
External penetration testing					X	Q3
Internal penetration testing					X	Q3
Data encryption key rotation					X	Q3

APPENDIX O – MANAGEMENT OF CONNECTED ENTITIES FORM

Company Name	Connection type and accessed system	Requested connection date	Requested connection time	Reason	Authorized by Manager/Title	Time Out
Mindshift Commack NY	VPN network tunnel	Permanent Connection	Permanent Connection	Access to hosting center	Vicky Mihal/Director of Infrastructure	N/A
Mindshift Minneapolis, MN	VPN network tunnel	Permanent Connection	Permanent Connection	Transfer of data	Vicky Mihal/Director of Infrastructure	NA
Scranton AWS US-EAST 1	VPN network tunnel	Permanent Connection	Permanent Connection	Access to hosting center	Vicky Mihal/Director of Infrastructure	NA
Mindshift MN to AWS US-EAST 1	VPN network tunnel	Permanent Connection	Permanent Connection	Access to hosting center	Vicky Mihal/Director of Infrastructure	NA
Contact US	VPN network tunnel	Permanent Connection	Permanent Connection	Access to Penn Foster Systems	Vicky Mihal/Director of Infrastructure	NA

APPENDIX R – MOBILE DEVICE POLICY

R.1 – Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to utilize a company owned or privately owned mobile device that is capable of connecting to a computer network outside of the direct control of Penn Foster. This mobile device policy applies to, but is not limited to all devices and accompanying media that fit the definition of Mobile Electronic Devices (see Section 5).

R.2 – Employees/Departments Affected

This procedure impacts all employees within the company who are issued or use a company owned Mobile Electronic Device. This policy also includes all employees who use or expense a personal Mobile Electronic Device for company purposes.

R.3 – Enforcement

Any employee that violates this policy may be subject to disciplinary action, up to and including termination.

R.4 - Definitions

Mobile Electronic Devices (MEDs) are small portable computing devices. Examples of these devices include:

- iPhones
- Wireless Smartphone
- Cellular/mobile telephones
- Personal Digital Assistants (PDAs)
- Any other mobile device capable of storing corporate data and connecting to a computer network.

R.5 – Responsibilities

Penn Foster Information Technology Department

The VP of IT and Enterprise Data Services, The Security Officer, and Mobile Electronic Device Administrators within Penn Foster's IT department will determine the security risks involved in deploying and using Mobile Electronic Devices. They will develop and maintain standards, policies, procedures and practices for the purpose of limiting corporate risk.

End User

The end user will recognize the vulnerability of the Mobile Electronic Devices and take the appropriate precautions to keep the device safe and secure. They will follow the following procedures outlined in this policy and agree to abide by this policy by signing it.

R. 6 – Procurement

A.) Company Issued Mobile Electronic Devices

1. Only the appropriate administrator within Penn Foster Information Technology department may order Mobile Electronic Devices (MEDs).
2. Employees working for Penn Foster and requesting a MED should fill out the attached device requisition form (attached).
3. Company issued Mobile Electronic Devices will be limited to those offered on the form unless approval is received from executive level management.
4. Personal telephone numbers will not be ported in, or ported off of the company MED plan unless approval is received from executive level management.

B.) Personal Mobile Electronic Devices

1. Employees may use a personal Mobile Electronic Device for business use.
2. Employees should acquire the allowed reimbursement amount for their business use from their hiring manager.
3. Employee reimbursement is the sole responsibility of the employee as outlined in that individuals expense policy.
4. Employees will be required to adhere to Penn Foster's Mobile Electronic Device Policy and pay special attention to the data security policies outlined.
5. Personal telephone numbers will not be ported in, or ported off of the company MED plan unless approval is received from executive level management.

R.7 - Physical Security

1. Employees are responsible to take proper care of company issued devices assigned to them to lower the chance of the being lost, stolen, or broken.
2. Company issued MEDs should be in a protective skin or case.
3. Employees may be responsible for the cost to repair or replace a mobile electronic device if the damage or loss is due to negligence or misconduct.
4. Penn Foster does not carry insurance and replacement costs can be up to $650.00.
5. Employees should not seek replacement of company issued MEDs prior to their renewal dates.

6. Upon separation from the company, all MEDs and accessories, including chargers will be returned to Penn Foster's IT Department.

R. 8 - Data Security

1. Employees are responsible to protect their personal or company issued Mobile Electronic Device with a passcode.
2. Employees are responsible to safeguard their MED passcodes.
3. Smartphones should have their data encryption features enabled.
4. Employees using personal MEDs may only use Penn Foster's Wireless Guest Network.
5. Employees must report any lost phone, personal or company issue, to Penn Foster's IT Department.
6. Penn Foster reserves the right to use software that will track the use of a stolen MED.
7. Employee must report any International travel plans in a timely fashion to Penn Foster IT so appropriate plan modifications can be made to company issued MEDs.
8. Employees should always use data and roaming with "best cost" measures in mind.
9. Employees should not use 411 or call completion fee based services excessively.
10. Employees are not permitted to download ringtones that have associated fees on a company issued MED.
11. Employees are not permitted to download applications or games that have associated fees on a company issued MED.
12. Company issued MEDs should be used for business purposes.
13. Company issued MEDs may be used to communicate with family while traveling on business or in case of an emergency.
14. Personal software, data, documents, images, videos, and music should not be stored on a company issued device.
15. No effort will be made to backup, restore, export or return any personal oftware, data, documents, images, videos, or music.
16. Penn Foster IT has the right to examine the contents of any MED, company issued, or personal, without knowledge or permission of the employee.
17. Along with the company owed device, the company also owns its associated phone number, email address, and any data stored on it.
18. Employees must update the operating system version on their device as determined by the IT department.