PCI Data Security and Classification Standards Summary

Data security should be a key component of all system policies and practices related to payment acceptance and transaction processing. As customers seek out merchants that are reputable and reliable, they expect assurance that their account information is being guarded and their personal data is safe.

Payment Card Industry (PCI) Compliance

To comply with regulations concerning credit cards, you must follow the PCI Data Security Standards, which are summarized below. See the actual standards posted on the PCI Standards Council site at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

References to policies are addressed at the system level. It is sufficient for each merchant to indicate in their departmental policies that they adopt all policies related to PCI compliance. To the extent a department's policies must differ from these policies, the exception must be clearly justified in the department's policy manual and the exception policy clearly articulated.

PCI Data Security Standards	
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored data
	4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software
	6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

Non-technical PCI standards are discussed in greater detail below. All PCI standards are considered requirements, unless otherwise noted.

Protect Stored Data

Do not store cardholder data unless absolutely necessary. Merchants can obtain cardholder data from Paymentech and credit card accounts should not be included with credit card journals, so most departments should not need to store this information.

If it is necessary to store cardholder data, the merchant must follow the requirements below:

- Keep cardholder information storage to a minimum.
- Retain data consistent with the system's records retention policy for category 4 data (fiscal records).
- Shred paper documents using approved destruction methods (minimally cross-cut shredding).
- Delete electronic files.
- Destroy (shred, crush or degauss using DoD type overwrite processes) any computer hard drive disposed of that contained credit card data.
- Do not store sensitive authentication data (CVV2, CVC2, PIN data) subsequent to authorization (not even encrypted).
- Do not store contents of magnetic stripe on back of card except name, PAN and expiration date. (Both Track 1 and Track 2).
- Do not store card validation code, which is a three or four digit code on back of card (e.g., CVV2 and CVC2 data).
- Do not store the PIN Verification Value (PVV).
- Mask the account number when displayed (first 6 digits and last 4 digits are the maximum number to be displayed). This does not apply to employees who need to see full account number.
- Render sensitive cardholder data (the account number at a minimum) unreadable anywhere it is stored electronically. (See component Information Technology Division for encryption techniques.)
- Protect encryption keys against disclosure and misuse.
    - Restrict access to keys to fewest number of individuals necessary.
    - Store keys securely in fewest possible locations and forms.
- Document and implement all encryption key management processes and procedures
    - Generation of strong keys (only industry tested and accepted algorithms allowed. No "proprietary" algorithms from vendor products should be accepted).
    - Secure key distribution.
    - Secure key storage.
    - Periodic key changes.

- Destruction of old keys.
- Split knowledge and dual control of keys (so 2 or 3 people need to work together to reconstruct the entire key).
- Prevention of unauthorized substitution of keys.
- Replacement of known or suspected compromised keys.
- Revocation of old or invalid keys.
- Requirement that key custodians sign a form acknowledging their key-custodian responsibilities.

Authorization Numbers

After successfully processing a transaction, you are returned an authorization number. This is unique per transaction and has no intrinsic value of its own. It is safe to store this value, write it to logs, present it to staff and email it to the customer.

Handling Recurring Payments

One of the few business reasons for storing credit card numbers is recurring payments. However, you have several responsibilities if you support recurring payments:

- You must follow the terms of your merchant agreement. Most merchant agreements require you to have original signed standing authorizations from credit card holders. This bit of signed paper will help you if the customer challenges your charges.
- If you store whole credit card numbers electronically, PCI guidelines require the numbers to be encrypted.
- Limit the term of the recurring payment to no more than one year, particularly if you have “cardholder not present” (CNP) transactions.
- Expunge the credit card details as soon as the agreement is finished.
- Card-not-present data such as CVV2, CVC2 and PIN numbers cannot be stored for recurring payments.

Encrypt Transmission of Cardholder Data and Sensitive Information Across Public Networks

- Use strong encryption techniques when transmitting cardholder data across public networks. (See component Information Technology Division for encryption techniques.)
- Never send cardholder data via unencrypted email.

Use and Regularly Update Anti-Virus Software

- Deploy anti-virus mechanisms on all systems commonly affected by viruses (e.g., PC’s and servers) that store, process, or transmit credit card information.

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

Restrict Access to Data by Business Need-to-Know

- Limit access to computing resources and cardholder data to those individuals whose job requires access.
- Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.

Restrict Physical Access to Cardholder Data

- Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.
    - Use cameras to monitor sensitive areas. Audit this data and correlate with other entries. Store camera data for at least three months, unless otherwise restricted by law.
    - Restrict physical access to publicly accessible network jacks.
    - Restrict physical access to wireless access points, gateways, and handheld devices.
- Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder information is accessible.
- Make sure all visitors who enter areas where cardholder data is processed or maintained are:
    - Authorized before entering those areas.
    - Given a physical token (e.g., badge or access device) that expires, and that identifies them as non-employees.
    - Asked to surrender the physical token before leaving the facility or at the date of expiration.
- Where physical tokens are provided to visitors, use a visitor log to retain a physical audit trail of visitor activity. Retain this log for a minimum of three months, unless otherwise restricted by law. Minimally, logs should require name, company and authorizing employee. These logs should be used at entrances to all facilities where cardholder data is stored, processed or transmitted.
- Store media back-ups, if any, in a secure off-site facility, which may be either an alternate third-party or a commercial storage facility.

- Physically secure all paper and electronic media (e.g., computers, electronic media, networking and communications hardware, telecommunication lines, paper receipts, paper reports, and faxes) that contain cardholder information.

- Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information.

    - Media should be identifiable as confidential based on some process (such as specially coded bar labels, color coded tape media, or other marking which only an employee would understand identifies the media as confidential.

    - Send the media via secured courier or a delivery mechanism that can be accurately tracked.

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

- Maintain strict control over the storage and accessibility of media that contains cardholder information:

    - Properly inventory all media and make sure it is securely stored.

- Destroy media containing cardholder information when it is no longer needed for business or legal reasons:

    - Cross-cut shred, incinerate, or pulp hardcopy materials.

    - Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.

Information Security for Employees and Contractors

- Develop daily operational security procedures that are consistent with PCI Data Security Standards, such as:

    - User account maintenance procedures.

    - Log review procedures. Retain logs consistent with the system's records retention policy for category 2 data (automation records).

- Ensure the proper use of employee facing technology (such as wireless, Bluetooth, GPRS and modems) by all employees and contractors by ensuring policies address the following:

    - Explicit management approval.

    - Authentication for use of the technology.

- A list of all such devices and personnel with access.
- Labeling of devices with owner, contact information, and purpose.
- Acceptable uses of the technology.
- Acceptable network locations for these technologies.
- A list of company-approved products.
- Automatic disconnect of modem sessions after a specific period of inactivity.
- Activation of modems for vendors only when needed by vendors, with immediate deactivation after use.
- Storage of cardholder data on local hard drives, floppy disks or other external media via cut and paste, screen print and other printing functions is prohibited.

- Clearly define information security responsibilities for all employees and contractors.
- Assign to an individual or team the following information security management responsibilities:
  - Distribute security policies and procedures to appropriate employees.
  - Monitor and analyze security alerts and information, and distribute to appropriate personnel.
  - Follow the security incident response and escalation procedures in the Incident Response Plan to ensure timely and effective handling of all situations.
  - Administer user accounts, including additions, deletions, and modifications.
  - Monitor and control all access to data..
- Make all employees aware of the importance of cardholder information security.
- Screen potential employees via background checks, police record checks or credit history checks to minimize the risk of attacks from internal sources.
- Contractually require all third parties and applications with access to cardholder data to adhere to payment card industry security requirements. At a minimum, the agreement should address:
  - Acknowledgement that the 3rd party is responsible for securing cardholder data to PCI standards while in their possession.
  - Third parties must be willing to provide evidence on a regular basis to show cardholder data is protected to PCI standards.

- Adhere to the Incident Response Plan. Be prepared to respond immediately to a system breach.
    - UHS Information Technology will coordinate an annual test of the incident response plan.
    - Designate specific personnel to be available on a 24/7 basis to respond to alerts.
    - Provide appropriate training to staff with security breach response responsibilities.
    - Include alerts from all appropriate sources to include intrusion detection, intrusion prevention, and file integrity monitoring systems.
    - The incident response plan will be revised according to lessons learned and to incorporate industry developments.