The HelpDesk LLC

Payment Card Industry (PCI) Compliance

Management Guidelines

About PCI Compliance
Payment Card Industry (PCI) compliance is a requirement for all businesses that accept credit cards. No business (small or large) is exempt from this guideline. Visa, MasterCard, Discover, American Express and other major credit card providers established the Security Standards Council (SSC) to determine what must be done to reduce vulnerabilities and protect credit card data. The result is a set of guidelines that all businesses must follow. A thorough and comprehensive document that explains the security standard in greater detail can be found at the following link:
http://thdurl.com/pciquickreference

The following pages of this document are a plain English summary that The HelpDesk LLC has compiled to assist our clients in knowing and understanding what is needed to comply. Note that The HelpDesk LLC document is not meant to be comprehensive or all inclusive. It is only a brief summary. We encourage our clients to obtain copies of the full guideline to read and study on their own.

12 Requirements Of PCI Compliance

1) **Use Firewalls—**Work with your network administrator to create a firewall that restricts traffic from untrusted networks. There should be no direct public access between the Internet and any system housing cardholder data. Any mobile device that has access should utilize personal firewall software.

2) **Diligent Use of Passwords—**Do not use vendor supplied default passwords. These are the first passwords that hackers try. Use data encryption where possible. If you utilize shared hosting, be sure that the host is encrypting data also.

3) **Protected Stored Cardholder Data—**As a general rule, only store the data, or parts of the data that is absolutely needed. Purge unneeded data on a regular basis. Do not store authorization data after authorization is received. Mask the personal account numbers (PAN) for all personnel that do not need to see the full number. Make the PAN unreadable (ie. encrypted,) anywhere that it is stored. Be sure to guard and protect any encryption keys that are used.

4) **Encrypted Transmissions**—This is a must when data is sent across any open or public network. Never send unprotected PANs across end-user messaging technologies.

5) **Use and maintain anti-virus software** on all systems affected by the use of this data. Be sure to not only use the software but keep it updated on a regular basis.

6) **Maintain secure systems and applications—**always use the most recently released software and be sure to keep it updated with patches and fixed that are regularly available. Whenever

changes are made, always follow the change procedures provided. If you are developing your own software always develop based on best practices regarding security. Be certain that your software is protected from all known attacks.

7) **Restrict Access to the Data—**Components and cardholder data access should be limited to only those who absolutely "need to know." In addition, access should be limited to only the parts of the data that are needed by that individual.

8) **Use Unique ID's—**All log-in's and ID's should be unique and specific to each individual that accesses the data. Implement a two-factor/layer login system for remote users. Render all passwords unreadable during storage and transmission, utilizing strong cryptography. Be sure to have proper user identification and authentication management for non-consumer users and administrators.

9) **Restrict Physical Access to Data—**Rooms where data is stored should be kept locked and secured with access limited to key personnel. Procedures should be in place to identify visitors from others with appropriate badges/ID in areas where cardholder data is stored. Media with cardholder data stored off-site should also be in a secure location. Strict controls should be in place over both the facility and the media. When media is no longer needed, it should be destroyed.

10) **Monitor and Test Networks to Find and Fix Vulnerabilities—**Logging mechanisms should be in place for effective tracking. System components and use of the system should be linked to users in those logs. Logs should be detailed by event, time, date, user, transaction type, success/failure, etc. Extensive audit trails should be implemented for all systems. Audit trails should be secure so that they cannot be altered. Audit logs should be reviewed daily by authorized personnel. Three months of audit trail history should be immediately available and stored for at least one year.

11) **Regularly Test Security Systems and Processes—**Internal and external network vulnerability scans should be conducted quarterly or daily, particularly at points of wireless entry. In addition, internal and external penetration testing should be conducted annually. Network intrusion detection systems should be used at the perimeter of the cardholder data environment. Use file integrity monitoring tools to alert personnel of changes made to critical files.

12) **Develop and Maintain an Information Security Policy**—A comprehensive policy that addresses PCI compliance procedures must be disseminated to all employees. The policy should be reviewed at least once a year. Procedures for the proper use of critical technologies where cardholder data is entered, managed or maintained should be included. Responsibility for overall data security should be clearly assigned to a person or team. The responsibilities for how each employee handles the data should also be spelled out. The policy should include an incident response plan. New employees should be screened with background checks to minimize risk of attack from internal sources. If cardholder data is shared externally, policies and procedures on each entity's role in handling data should also be spelled out. The policy should also include an incident response plan.

Payment Card Industry (PCI) Compliance

Employee Guidelines

What Is PCI Compliance

PCI is an acronym for Payment Card Industry. The payment card industry is made up of major credit card issuers like Visa, MasterCard, Discover and Amex. All card issuers belong to an association called the Security Standards Council (SSC). The SSC has issued a set of guidelines for reducing credit card fraud. All businesses that accept credit cards must follow these guidelines. If the guidelines are not followed the businesses face very large fines and liabilities. This document is designed to help train and inform employees of the guidelines and how to follow them.

PCI Compliance Guidelines

1) **Credit Card Information Should Be Protected--**The first thing to remember is that credit card information should be protected. It is valuable and is similar to leaving cash on your desk. When your company receives credit card information by phone, Internet or other means, steps should be taken to keep the information under cover and out of sight from others. For example, do not leave credit card information in plain sight on your desk while you are away for extended periods of time. This increases the risk that visitors and unauthorized individuals may have access to it. For example, when you go home at night, and the cleaning crew comes in, credit card information should be locked up out of sight.

   Key Points

   - Only store data that is absolutely needed.
   - Be sure that data is in a locked cabinet or area of the office.
   - Always make sure data is stored in it's proper place at the end of the day.
   - Do not give customer credit card information to unauthorized employees.

2) **Diligently Use & Protect Passwords--**You should not use passwords that are easy for others to figure out. Do not use things like pet names or favorite colors. Do not use vendor supplied default passwords. These are the first passwords that hackers try. The network system password that your administrator has set up is a strong line of defense against credit card fraud when you use it properly! Passwords should be six or more characters and preferably some combination of letters and numbers. If your system uses case-sensitive letters, then use a combination of capital and lower case letters.

   Do not write your password on a sticky note and place it on your computer screen. Although this may be convenient for you and help you remember, it defeats the purpose of using passwords and keeping customer data protected.

3) **Proper Use Of The Computer & Security System--**Be sure to always properly use the computer, network and security system that your employer has put in place. Do not bypass security systems, disable virus scanning or other measures that will cause the security to fail.

Your employer has put these systems in place to protect you and your customers from fraud. When you use the system the way it was supposed to be used, you are also helping your customers avoid problems. It is important that you always use the system the way it was designed to be used.

Key points:

- Always use the computer system the way it was designed.
- Do not bypass or shut down security systems.
- Think of your clients/customers first

4) **Remind Those Around You of the Importance--**When your customers share their credit card data with you they expect that you will guard it from wrongful use. Sometimes those around us forget how important this is. You can be the one to remind them how much your customers and clients appreciate it. If you see credit card information unprotected, be sure to remind them of the importance of protecting your customers' data.

Key points:

- Think of your customers first.
- It's their information that you are protecting!
- Rally the support of your fellow workers to help in this effort.

5) **Follow Your Employer's Policies--**The Policies and Procedures that your employer has in place to prevent credit card fraud does three things: It protects you. If credit card fraud occurs and you have followed all of the procedures that were in place at the time, then you are not at fault. Next, the Policies protects your customers and clients. They are counting on you to protect their personal information. Following the Policies accomplishes that. Third, when you follow the Policies it protects your employer from serious fines. Your employer wants to stay in business. And, when they stay in business you still have a job. This makes you a vital part of the team. So following the Policies helps everyone win!

Key points:

- When you follow the Policy everyone wins:
- You, the customers and your employer!

6) **Alert Your Employer--**You are a vital member of the team in serving your customers and protecting their data. Because you are on the "front line" of service to the customers you are in an excellent position to not only make things happen, but also see what's happening. If you see things that don't seem right, or have creative ideas on ways to improve the process, speak up. Your employer expects you to be part of the process in properly serving customers and helping protect their information.

Key points:

- You are part of the Team! Speak up if you see:
- Vulnerabilities in the system, or
- Ways to improve the process of protecting customer data.

SMALL BUSINESS DATA SECURITY POLICY

PURPOSE

Our Company is committed to meeting the Data Security Standard of the Payment Card Industry Council. To that end, we have adopted the following security policies. This policy states requirements for the protection of such sensitive data according to the PCI Data Security Standard (Version 1.2 is current upon publication date of this policy).

OUR EMPLOYEES

This policy applies to all employees of [COMPANY NAME] and to all others given use of, or having access to, sensitive data.

This policy applies to sensitive data stored, processed and transmitted within or among any and all [COMPANY NAME's] information systems, whether individually controlled or shared, stand-alone or networked, and all computer systems and communication facilities owned, leased and operated by or on behalf of [COMPANY NAME]. This includes, at minimum, networking devices, mainframes, workstations, personal computers, smart phones, telephones, wireless devices and any associated peripheral equipment and software.

OUR BUILDINGS

Restrict Physical Access to Cardholder Data

Physical access to all credit-card data must be restricting, using appropriate building access controls to limit and monitor physical access to restricted credit-card data. Required measures include:

- Video monitoring of all areas where credit-card data is handled or stored;
- Storage of access log data for at least three months;
- Restrict physical access to publicly accessible computer network access points, including wireless access points;
- Visitors must be authorized before entering areas where credit-card data is handled or stored;
- Visitors must receive a form of physical identification that identifies them as visitors;
- A visitor log to maintain a physical audit trail of visitor activity. The log must be retained for a minimum of three months;
- Secure destruction of media containing credit-card data:
    - Paper: cross-cut shred, incinerate or pulp;
    - Electronic media: securely overwrite data, degauss, shred or otherwise completely destroy

OUR DOCUMENTS

[COMPANY NAME] maintains a variety of documents in the course of conducting daily business. Some of these documents may contain sensitive data or references to information that could provide access to sensitive data. Access to these documents is explicitly restricted to a "need to know" basis, and all unauthorized access or sharing of restricted information may be met with disciplinary and/or legal action.

OUR NETWORK

Install and Maintain a Firewall Configuration to Protect Data

Use a firewall at each Internet connection point on the company network.

- Develop and document a firewall configuration that denies all traffic from nontrusted networks and hosts, except for those protocols necessary for the secure transmission of credit-card data;
- Develop and maintain a list of network services and ports required for business purposes;
- Develop and maintain a network diagram with all connections to credit-card-related data, including a diagram for any wireless networks
- List justifications for any open protocols aside from hypertext transfer protocol (HTTP), secure sockets layer (SSL), secure shell (SSH) and virtual private network (VPN);
- Develop and maintain documentation that justifies any open firewall ports that could be considered a risk to network security;
- Develop and maintain a router-configuration diagram that demonstrates restricted access between public networks and any company computer system that stores credit-card data;
- Document personal computer firewall requirements;
- Prohibit direct public access between external networks and any system component that stores credit card related data (for example, databases, logs and trace files);
- Document all firewall rule sets.

Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Prohibit the use of vendor-supplied default settings and remove unnecessary functionality supplied by vendors and prepackaged software solutions that could create a security vulnerability.

- Always change vendor-supplied default settings before installing a system on the company network, including passwords, simple network management protocol (SNMP) community strings and deletion of unnecessary system accounts;
- Document standards for system builds;
- Document all enabled services, daemons and protocols on servers;
- Document all security parameters enabled on each server;
- Remove any unnecessary functionality, such as features, scripts, drivers, file systems and unnecessary Web servers;
- Document all applications installed on each company server;

- Allow only ONE primary function for each company server (example: Web servers, database servers and domain name system (DNS) services should NOT be implemented in any combination on the same server).

OUR COMPUTERS

Encrypt Transmission of Cardholder Data and Sensitive Information Across Public Networks

Transmission of credit-card data across open, public networks must be encrypted, including the use of e-mail encryption software by employees. Cryptography is to be applied as defined by the PCI DSS 1.2 Glossary.

- Maintain a documented list of URL(s) used for transactions or passing credit-card-related information.
- Encrypt all wireless traffic used for transmitting credit-card data.
- Encrypt credit-card data transmissions using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never use wired equivalent privacy (WEP) to protect confidentiality and access to a wireless network.
- Document any current e-mail encryption software being used by employees, if any credit-card data is to be transmitted via e-mail communications.

Use and Regularly Update Anti-Virus Software

Use anti-virus software or programs and regular anti-virus signature updates, and document this use.

- Document current use of virus protection software;
- Document that installed anti-virus programs can detect and protect against other forms of malicious software (malware), including spyware and adware;
- Maintain a copy of anti-virus logs and reports.

Develop and Maintain Secure Systems and Applications

Develop and maintain secure computer systems and software applications, and ensure that security measures are included for new or upgraded systems and applications.

- Maintain separate development, test and production (live) environments.
- Separate the duties of those who work on the development, test and production environments.
- Remove all custom accounts, usernames and passwords before a system goes live.
- Do not use “live” data from production systems for testing or development of new systems.
- Remove all test data and test accounts from production systems before they go live.

- Keep a copy of the last formal code review report for in-house created systems and applications.

Restrict Access to Data to a Need-to-Know Basis

Access to all credit-card data must be restricted strictly on a need-to-know basis, limiting access to only those employees who must access the data to perform their job duties.

- Install and maintain access controls that restrict computer user access to only those systems and resources required for performing their jobs.
- Maintain access logs that show which employees had access to what data, and when, for all computer systems.

Assign a Unique ID to Each Person With Computer Access

Each person with computer access MUST be assigned a unique account ID with a password known only to that individual.

- Passwords must change every 90 days.
- Passwords must be a minimum of 7 characters, containing numeric, alphabetic and special characters.
- New passwords cannot be the same as previous passwords.
- If a user tries to log in but is unsuccessful after six attempts, that user account must be automatically locked out for 30 minutes or until a system administrator is contacted to manually unlock the account.
- Set a computer idle lock out time of 15 minutes and require a password to gain access to the computer again.
- Maintain a list of any inactive accounts.
- Keep a copy for six months of all employees with computer access.
- Ensure that no shared accounts and passwords exist on any computer systems.

Track and Monitor all Access to Network Resources and Cardholder Data

All access to [COMPANY NAME's] network and cardholder data must be tracked and monitored for any signs of suspicious or unauthorized activity.

- Capture system logs and maintain log records for 12 months.
- Monitor system logs daily or use automated alerting mechanisms to ensure that suspicious or unauthorized activity is quickly detected.
- Respond swiftly to any indications of suspicious or unauthorized activity.

OUR DATA

Protect Stored Data

Stored credit-card data must be protected from unauthorized use at all times.

- Do not allow the display of personal account numbers in full; display of the first six and/or the last four digits is permissible.
- If personal account numbers must be stored, they must be protected in one of four ways:
    - Strong encryption with secure encryption key management
    - Truncation of account number
    - Strong one-way hash
    - Use of index tokens and pads

OUR SERVICE PROVIDERS

Closely manage all third-party service providers and partners to ensure that all business conducted on [COMPANY NAME]'s behalf is performed to the PCI DSS requirements and standards.

- All new contracts must be reviewed from a security perspective to ensure that services provided by third parties will be rendered in a PCI-compliant manner.
- All existing contracts should be reviewed at least annually and updated as needed to ensure that third-party services continue to meet PCI requirements.
- Where possible, conduct an on-site inspection of any potential new third party or partner and document the state of secure data practices.

OUR SECURITY PROGRAM

Regularly Test Security Systems and Processes

All [COMPANY NAME] systems must be tested quarterly to ensure that security systems and processes are in place and performing as needed.

- Develop and maintain a security-breach-response plan, and test the plan at least annually.
- Perform internal and external vulnerability scans of all systems connected to the cardholder data environment, per current PCI DSS requirements.
- Ensure that all credit-card data is completely destroyed (degauss disks, shred paper) once the data or the medium that the data resides upon is no longer needed for clear business purposes.

Maintain a Policy That Addresses Information Security

The [COMPANY NAME] information security policy is to be reviewed and updated as needed at least annually by [COMPANY NAME] management.

- [COMPANY NAME] will train all new employees on data security practices to a level appropriate for their job positions.
- All employees will receive security awareness training at least annually, and all employees must sign this policy to indicate that the policy is understood and will be abided by.

- Background checks are suggested for all employees with access to one credit-card number at a time, and mandatory for all employees with access to multiple credit card numbers at a time in performing their duties.
- When an employee moves to a new position within [COMPANY NAME], a review of the employee's new role and what sensitive data access that the new role requires will be conducted. Access to sensitive data may be granted or revoked based on need-to-know basis according to the new job duties. A background check may also be required for a current employee moving from a role where no access to sensitive data was required to a role that necessitates access to sensitive data.