



Credit Card Processing & Payment Card Industry Standard

Background

The Payment Card Industry (PCI) has created requirements for protecting payment card information, including information on computers which process and store credit card and other payment card information. These requirements became effective June 30, 2005. Merchants must adhere to these standards to limit their liability and continue to process payments using payment cards.

Ignoring the PCI Compliance standard is risky. Retailers can be fined and even lose card processing privileges. Security breaches can damage a company's brand and reputation and lead to financial losses.

PCI Data 101

All computers and electronic devices at the merchant involved in processing payment card data are impacted by the PCI Data Security Standard. This includes servers that store payment card numbers, workstations that are used to enter payment card information into a central system (e.g., ordering tickets over the phone), and any computers through which the payment card information is transmitted.

The merchant and all units that process payment card data have a contractual obligation to adhere to the PCI Data Security Standard (PCI-DSS). Management and Information Technology needs to work with all departments to assure compliance.

To help meet the Payment Card Industry requirements, COMMON_d recommends the following:

Best Practice

1. Identify all devices involved in credit card processing such as production, test/development, backup servers, domain controllers, load balancers, and others.

2. Assess all IP address or static DHCP used for computers involved in credit card processing.
3. Apply security settings to servers and other operating system platforms similar to the settings in desktops. This includes installing antivirus software with anti-spyware and adware software.
4. Review what software is running on the computer and remove software not needed.
5. Each open port must have a valid business reason.
6. All nodes/workstation/ip/servers/printers involved in credit card processing need to be in a **secured** vlan.
7. Review what software is running on the computer and remove software not needed. General purpose web browsing and e-mail should not be allowed.
8. Design a workable Security Policy to be used to determine the secure vlan policy for your network.
9. Minimize the use of wireless for credit card processing.
10. Web servers should run SSLv3 with strong encryption enabled, and SSLv2 should be disabled.
 - a. Typically, for Apache/mod_ssl, httpd.conf or ssl.conf should have the following lines:
 - i. SSLProtocol -ALL +SSLv3 +TLSv1
 - ii. SSLCipherSuiteALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
 - b. For Apache/apache_ssl include the following line in the configuration file (httpsd.conf):
 - i. SSLRequireCipher
 - ii. ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
11. For Microsoft IIS, see How to Disable SSLv2 on IIS : Microsoft Knowledge Base Article - 187498

12. Use a secure deletion program to wipe the disk drive when terminating credit card processing.

13. Use the proxy to download operating system updates and anti-virus live updates.

ABC to PCI Compliance:

According to industry experts, the best way to achieve and maintain compliance is through a strategic, holistic approach that encompasses improved operational efficiency through:

