Payment Card Industry Data Security Standard (PCI DSS)
What is PCI SSC?

- A 12 year old independent industry standards body providing oversight of the development and management of Payment Card Industry Security Standards on a global basis
- 2004 Founding multi-national acceptance brand members:
  - American Express
  - Discover Financial
  - JCB International
  - MasterCard Worldwide
  - Visa, Inc.
# Card Payment Brands

- Each payment brand develops and maintains its own PCI DSS compliance programs in accordance with its own security risk management policies

<table>
<thead>
<tr>
<th>Card Payment Brand</th>
<th>Compliance Program</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>American Express:</strong></td>
<td>Data Security Operating Policy (DSOP)</td>
</tr>
<tr>
<td><strong>Discover:</strong></td>
<td>Discover Information Security Compliance (DISC)</td>
</tr>
<tr>
<td><strong>JCB:</strong></td>
<td>Data Security Program</td>
</tr>
<tr>
<td><strong>MasterCard:</strong></td>
<td>Site Data Protection (SDP)</td>
</tr>
<tr>
<td><strong>Visa Inc.: Visa Europe:</strong></td>
<td>Cardholder Information Security Program (CISP) Account Information Security (AIS) Program</td>
</tr>
</tbody>
</table>
Payment Industry Terminology

Issuer → Payment Brand Network → Acquirer → Merchants → Cardholders
Payment Industry Terminology

- **Cardholder**
  - Customer purchasing goods either as a “Card Present” or “Card Not Present” transaction
  - Receives the payment card and bills from the issuer

- **Issuer**
  - Bank or other organization issuing a payment card on behalf of a Payment Brand (e.g. MasterCard & Visa)
  - Payment Brand issuing a payment card directly (e.g. Amex, Discover, JCB)

- **Merchant**
  - Organization accepting the payment card for payment during a purchase
Payment Industry Terminology

Acquirer

- Bank or entity the merchant uses to process their payment card transactions
- Receive authorization request from merchant and forward to Issuer for approval
- Provide authorization, clearing and settlement services to merchants
- Acquirer is also called:
  - Merchant Bank
  - ISO (sometimes)
  - Payment Brand - Amex, Discover, JCB
  - Never Visa or MasterCard
Card Processing - Authorization

• Merchant requests and receives authorization to allow the purchase to be conducted
• Authorization Code is provided

1. Cardholder swipes card at merchant
2. Merchant’s bank asks processor to determine cardholder’s bank
3. Processing network determines cardholder’s bank and requests approval for purchase
4. Cardholder's bank approves purchase
5. Processor sends approval to merchant's bank
6. Merchant’s bank sends approval to merchant
7. Cardholder completes purchase and receives receipt

Authorization (Time of Purchase)
Card Processing - Clearing

- Acquirer and Issuer exchange purchase information

Merchant’s bank sends purchase information to the Processor network

Processor sends purchase information to cardholder’s bank, which prepares data for cardholder’s statement

Processor provides complete reconciliation to merchant’s bank

Clearing (Usually within one day)
Card Processing - Settlement

- Merchant’s bank pays merchant for cardholder purchase
- Cardholder’s bank bills cardholder

1. Cardholder’s bank sends payment to processor

2. The processor’s settlement bank sends payment to merchant’s bank

3. Merchant’s bank pays merchant for cardholder’s purchase

4. Cardholder’s bank bills cardholder

Settlement (Usually within two days)
What is Cardholder Data?

<table>
<thead>
<tr>
<th>Account Data</th>
<th>Sensitive Authentication Data includes:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cardholder Data includes:</strong></td>
<td>• Full magnetic stripe data or equivalent on a chip</td>
</tr>
<tr>
<td>• Primary Account Number (PAN)</td>
<td>• CAV2/CVC2/CVV2/CID</td>
</tr>
<tr>
<td>• Cardholder Name</td>
<td>• PINs/PIN blocks</td>
</tr>
<tr>
<td>• Expiration Date</td>
<td></td>
</tr>
<tr>
<td>• Service Code</td>
<td></td>
</tr>
</tbody>
</table>

- Many people refer to **ALL** account data simply as “Cardholder Data”.
- Remember, PCI DSS requirements are applicable wherever Primary Account Number (PAN) or Sensitive Authentication Data (SAD) is stored, processed, or transmitted.
- Account Data includes all of the information printed on the physical card as well as the data on the magnetic stripe or chip
- Sensitive Authentication Data cannot be stored after authorization.
- Encrypting Cardholder Data or Sensitive Authentication Data does **NOT** necessarily remove it from scope.
**Track 1 vs. Track 2 Data**

• Payment Cards use two tracks of payment data on the magnetic stripe:
  • Track 1
    – Contains all fields of both track 1 and track 2
    – Length up to 79 characters
  • Track 2
    – Provides shorter processing time for older dial-up transmissions
    – Length up to 40 characters
Track 1 Data
Track 2 Data

- PAN
- Separator
- Expiration Date
- Discretionary Data (including CVV/CVC)
- PIN Verification Data
- Service Code
How Does PCI DSS Apply to Chip Transactions?

• Merchants are not permitted to store the track equivalent data following authorization.
• Track equivalent data found on the chip differs from the track data found on the magnetic stripe as the chip track data contains a unique Chip CVV/CVC code.
• This prevents criminals producing cloned magnetic stripe cards from chip track data.
• However there is still sufficient information to allow criminals to use this data in a Card Not Present fraud.
“Persistent Storage” of Track Data Post Authorization is Never Permitted

• It is noncompliant to store full track data post-authorization, even if using:
  • Encryption
  • Password protection
  • Data scrambling/obfuscation
  • Masking
  • Proprietary data formats

• Exception:
  • Issuers and issuing processors may be permitted to retain sensitive authentication data if needed for business purposes
Track Data Location

• Track data can be found in a variety of data stores
• Typical location of track data storage include:
  • Databases
  • Flat files
  • Log files
  • Debug files
• Systems that commonly store track data:
  • POS systems
  • POS servers
  • Authorization servers

- WHAT IS SCOPE? Anything that Stores, Processes, or Transmits Cardholder Data (CHD) is “IN-SCOPE” for PCI.

- Lately, the push is to use encryption solutions to reduce the scope of the PCI Cardholder Data Environment (CDE).

- The PCI SSC has stated for many years that encrypted CHD where a merchant can’t gain ANY access to the keys used for encrypting the CHD is actually not CHD at all...

- In fact, it can be seen as “Out-of-Range”. This is how a P2PE or E2EE solution can greatly support a merchant’s ability to benefit from the scope reduction provided by the implemented solution.
Point-to-Point Encryption (P2PE) – Why did the PCI SSC create the P2PE Standard?

• 2010 – The PCI SSC wanted to provide a common set of requirements for existing or future solutions to protect cleartext Cardholder Data (CHD) from the “Swipe”, “dip”, “shove”, “drag”, “WHATEVER” at the Point-of-Interaction (POI) to the other end at a decryption point/area where the CHD can be “Read” in cleartext and then passed on, processed, etc. by an acquirer.
End-to-End-Encryption (E2EE) – What are the differences between P2PE and E2EE?

- P2PE is the name the council decided to use when coming up with the original draft standard. The name of the standard is immaterial really. The point of protecting cleartext CHD is the aim of both P2PE and E2EE. Using technology to do this is what both P2PE and E2EE solutions are designed to accomplish.

- However, when you compare P2PE and E2EE, there could be many differences in terms of “HOW” the E2EE provider manages their solution vs a validated P2PE provider. Why? Because the P2PE provider is following the P2PE standard.

19
The 12 MAIN PCI DSS Requirements/Sub-Requirements
Build and Maintain a Secure Network

In the past, theft of financial records required a criminal to physically enter an organization’s business site. Now, many payment card transactions (such as debit in the U.S. and “chip and pin” in Europe) use PIN entry devices and computers connected by networks. By using network security controls, entities can prevent criminals from virtually accessing payment system networks and stealing cardholder data.

**Requirement 1: Install and maintain a firewall and router configuration to protect cardholder data**

Firewalls are devices that control computer traffic allowed into and out of an organization’s network, and into sensitive areas within its internal network. Firewall functionality may also appear in other system components. Routers are hardware or software that connects two or more networks. All such devices are in scope for assessment of Requirement 1 if used within the cardholder data environment.

1.1 Establish firewall and router configuration standards that formalize testing whenever configurations change; that identify *all* connections to cardholder data (including wireless); that use various technical settings for each implementation; and stipulate a review of configuration rule sets at least every six months.

1.2 Build firewall and router configurations that restrict all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization’s network.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

The easiest way for a hacker to access your internal network is to try default passwords or exploits based on default system software settings in your payment card infrastructure. Far too often, merchants do not change default passwords or settings upon deployment. This is akin to leaving your store physically unlocked when you go home for the night. Default passwords and settings for most network devices are widely known. This information, combined with hacker tools that show what devices are on your network can make unauthorized entry a simple task – if you have failed to change the defaults.

2.1 Always change vendor-supplied defaults before installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.

2.2 Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified.

2.3 Encrypt using strong cryptography all non-console administrative access such as browser/web-based management tools.

2.4 Shared hosting providers must protect each entity’s hosted environment and cardholder data (details are in PCI DSS Appendix A: “Additional PCI DSS Requirements for Shared Hosting Providers.”)
Protect Cardholder Data

Cardholder data refers to any information printed, processed, transmitted or stored in any form on a payment card. Entities accepting payment cards are expected to protect cardholder data and to prevent their unauthorized use – whether the data is printed or stored locally, or transmitted over a public network to a remote server or service provider.

Requirement 3: Protect stored cardholder data

In general, no cardholder data should ever be stored unless it’s necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored. If your organization stores PAN, it is crucial to render it unreadable (see 3.4, and table below for guidelines).

3.1 Limit cardholder data storage and retention time to that required for business, legal, and/or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.

3.2 Do not store sensitive authentication data after authorization (even if it is encrypted). See guidelines in table below. Issuers and related entities may store sensitive authentication data if there is a business justification, and the data is stored securely.

3.3 Mask PAN when displayed; the first six and last four digits are the maximum number of digits you may display. Not applicable for authorized people with a legitimate business need to see the full PAN. Does not supersede stricter requirements in place for displays of cardholder data such as on a point-of-sale receipt.

3.4 Render PAN unreadable anywhere it is stored – including on portable digital media, backup media, in logs, and data received from or stored by wireless networks. Technology solutions for this requirement may include strong one-way hash functions of the entire PAN, truncation, index tokens with securely stored pads, or strong cryptography. (See PCI DSS Glossary for definition of strong cryptography.)
3.5 Protect any keys used for encryption of cardholder data from disclosure and misuse.

3.6 Fully document and implement all appropriate key management processes and procedures for cryptographic keys used for encryption of cardholder data.

### Guidelines for Cardholder Data Elements

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Render Stored Account Data Unreadable per Requirement 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cardholder Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Service Code</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Account Data</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Magnetic Stripe Data(^2)</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
<tr>
<td>CAV2/CVC2/CVV2/CID</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
<tr>
<td>PIN/PIN Block</td>
<td>No</td>
<td>Cannot store per Requirement 3.2</td>
</tr>
</tbody>
</table>

---

1. Sensitive authentication data must not be stored after authorisation (even if encrypted).
2. Full track data from the magnetic stripe, equivalent data on the chip, or elsewhere.
Requirement 4: Encrypt transmission of cardholder data across open, public networks
Cyber criminals may be able to intercept transmissions of cardholder data over open, public networks so it is important to prevent their ability to view these data. Encryption is a technology used to render transmitted data unreadable by any unauthorized person.

4.1 Use strong cryptography and security protocols such as SSL/TLS, SSH or IPSec to safeguard sensitive cardholder data during transmission over open, public networks (e.g. Internet, wireless technologies, Global System for Mobile communications [GSM], General Packet Radio Service [GPRS]). Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. The use of WEP as a security control is prohibited.

4.2 Never send unprotected PANs by end user messaging technologies.

Maintain a Vulnerability Management Program
Vulnerability management is the process of systematically and continuously finding weaknesses in an entity’s payment card infrastructure system. This includes security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

Requirement 5: Use and regularly update anti-virus software or programs
Many vulnerabilities and malicious viruses enter the network via users’ e-mail and other online activities. Anti-virus software must be used on all systems affected by malware to protect systems from current and evolving malicious software threats.

5.1 Deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers).

5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.
Requirement 6: Develop and maintain secure systems and applications

Security vulnerabilities in systems and applications may allow criminals to access PAN and other cardholder data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation. Entities should apply patches to less-critical systems as soon as possible, based on a risk-based vulnerability management program. Secure coding practices for developing applications, change control procedures and other secure software development practices should always be followed.

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

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Risk rankings should be based on industry best practices and guidelines. Ranking vulnerabilities is a best practice that will become a requirement on July 1, 2012.

6.3 Develop software applications (internal and external, and including web-based administrative access) in accordance with PCI DSS and based on industry best practices. Incorporate information security throughout the software development life cycle.

6.4 Follow change control processes and procedures for all changes to system components.

6.5 Develop applications based on secure coding guidelines and review custom application code to identify coding vulnerabilities. Follow up-to-date industry best practices to identify and manage vulnerabilities.

6.6 Ensure all public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications.
Implement Strong Access Control Measures

Access control allows merchants to permit or deny the use of physical or technical means to access PAN and other cardholder data. Access must be granted on a business need to know basis. Physical access control entails the use of locks or restricted access to paper-based cardholder records or system hardware. Logical access control permits or denies use of PIN entry devices, a wireless network, PCs and other devices. It also controls access to digital files containing cardholder data.

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. Need to know is when access rights are granted to only the least amount of data and privileges needed to perform a job.

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

7.2 Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.

Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Requirements apply to all accounts, including point of sale accounts, with administrative capabilities and all accounts with access to stored cardholder data.

8.1 Assign all users a unique user name before allowing them to access system components or cardholder data.
8.2 Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric.

8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. For example, use technologies such as remote authentication and dialin service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication. Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication.

8.4 Render all passwords unreadable during storage and transmission, for all system components, by using strong cryptography.

8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components.

**Requirement 9: Restrict physical access to cardholder data**

Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hardcopies, and should be appropriately restricted. “Onsite personnel” are full- and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity’s premises. “Visitors” are vendors and guests that enter the facility for a short duration - usually up to one day. “Media” is all paper and electronic media containing cardholder data.

9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.
9.3 Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained; given a physical token that expires and that identifies visitors as not onsite personnel; and are asked to surrender the physical token before leaving the facility or at the date of expiration.

9.4 Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name and company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law.

9.5 Store media back-ups in a secure location, preferably off site.

9.6 Physically secure all media.

9.7 Maintain strict control over the internal or external distribution of any kind of media. Classify media so the sensitivity of the data can be determined.

9.8 Ensure that management approves any and all media moved from a secured area, especially when media is distributed to individuals.

9.9 Maintain strict control over the storage and accessibility of media.

9.10 Destroy media when it is no longer needed for business or legal reasons.

Regularly Monitor and Test Networks

Physical and wireless networks are the glue connecting all endpoints and servers in the payment infrastructure. Vulnerabilities in network devices and systems present opportunities for criminals to gain unauthorized access to payment card applications and cardholder data. To prevent exploitation, organizations must regularly monitor and test networks to find and fix vulnerabilities.
Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong. Determining the cause of a compromise is very difficult without system activity logs.

10.1 Establish a process for linking all access to system components to each individual user – especially access done with administrative privileges.

10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of the audit logs; creation and deletion of system-level objects.

10.3 Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.

10.4 Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time.

10.5 Secure audit trails so they cannot be altered.

10.6 Review logs for all system components related to security functions at least daily.

10.7 Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.
Requirement 11: Regularly test security systems and processes

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security is maintained over time. Testing of security controls is especially important for any environmental changes such as deploying new software or changing system configurations.

11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. Typical methods are wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, pass four consecutive quarterly scans as a requirement for compliance. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes may be performed by internal staff.

11.3 Perform external and internal penetration testing, including network- and application-layer penetration tests, at least annually and after any significant infrastructure or application upgrade or modification.

11.4 Use network intrusion detection systems and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.

11.5 Deploy file integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly.
Maintain an Information Security Policy

A strong security policy sets the tone for security affecting an organization’s entire company, and it informs employees of their expected duties related to security. All employees should be aware of the sensitivity of cardholder data and their responsibilities for protecting it.

Requirement 12: Maintain a policy that addresses information security for all personnel

12.1 Establish, publish, maintain, and disseminate a security policy that addresses all PCI DSS requirements, includes an annual process for identifying vulnerabilities and formally assessing risks, and includes a review at least once a year and when the environment changes.

12.2 Develop daily operational security procedures that are consistent with requirements in PCI DSS.

12.3 Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.

12.5 Assign to an individual or team information security responsibilities defined by 12.5 subsections.

12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.

12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. Example screening includes previous employment history, criminal record, credit history, and reference checks.
Thank You For Attending

Any Questions?