



PCI Data Requirements – PCI DSS

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.

Ongoing development of the standard will provide for feedback from the Advisory Board and other participating organizations. All key stakeholders are encouraged to provide input, during the creation and review of proposed additions or modifications to the PCI DSS.



The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Build and Maintain a Secure Network

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

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

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

Requirement 9: Restrict physical access to cardholder data

Logistica Solutions Inc - 3855 E La Palma Ave - Suite 104 - Anaheim, CA 92870 - 714-238-3209 - 877-314-1618

<http://www.ecomstor.com> - <http://www.integrazon.com> - <http://www.interpristor.com> - <http://www.interpriseo.com>



Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

To further the adoption of the PCI DSS, the PCI Security Standards Council defines credentials and qualifications for QSAs and ASVs. The PCI Security Standards Council also manages a global training and certification program for QSAs and ASVs, and will publish a directory of certified providers on this Web site.

Merchant Sensitive Information – PCI Requirements

Summary: Credit/debit card payments must be processed in an efficient, consistent, secure, and controlled manner in compliance with the Payment Card Industry Data Security Standard. Compliance is the entire corporation's responsibility with duties and accountability assigned at every level of the payment process.

1. Payment information is defined as credit card number, credit card expiration date, credit card ccv number, social security number, and credit card name.
2. All database transactions will go through one layer of software, consisting of two modules, one for the public side and another for the administration side.
3. All database transactions involving payment information will be logged into a database table for research of attacks and historical research reporting.
4. All database queries will be monitored for Sql injection attacks. If found, such queries will terminate the web page with an error message.
5. Credit card numbers will be encoded (using Php pack/unpack functions) within the database to prevent casual viewing by database personnel and provide another layer of security if the database security is lost.
6. All web software will be reviewed to prevent display of credit card numbers.
7. Database access will be limited by firewall to the Ecomstor webserver.
8. The Ecomstor webserver will have a firewall to protect against all but legitimate web requests
9. All transactions to payment gateways will use an SSL transport mechanism.



10. New payment gateways must provide a SSL transport mechanism and a testing methodology.
11. Clients who buy and download the software will receive a security review by Logistica personnel at time of purchase at the buyer's request. System changes recommended will be the responsibility of the client.
12. Clients at any time may purchase a review of their server's security by Logistica personnel.
13. All addon software will be adapted to go through the database layer (point 2 above)
14. All customer logins will be via an encoded layer.
15. A customer password strength process will be enforced to reduce hacking.
16. Customer passwords will be encoded to ensure their security within the database if a database breach should occur.
17. This document will be reviewed yearly and updated in light of experience by a software developer and network administrator. Results of such reviews will be read and signed by owners of Logistica Inc.

Prioritized Approach – PCI DSS 1.2

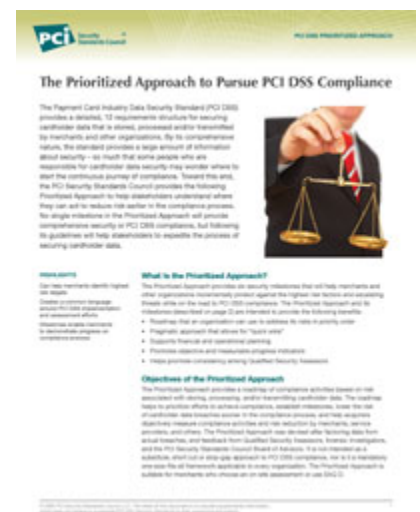
The Prioritized Approach provides guidance that will help merchants identify how to reduce risk to card holder data as early on as possible in their compliance journey. The tool groups together the requirements of PCI DSS 1.2 into six key milestones for merchants to consider in their card data security strategy.

The Prioritized Approach for PCI DSS 1.2 was created with input from the PCI SSC Board of Advisors, and informed by insight from real world results of data compromises shared by the assessment community. The Prioritized Approach offers guidance on how to focus PCI DSS implementation efforts in a way that expedites the security of cardholder data. It also

Helps businesses identify highest risk targets

Creates a common language around PCI DSS implementation efforts

Enables merchants to demonstrate progress on compliance process to key stakeholders – banks, acquirers, QSAs, others





Prioritized Approach Guide and Worksheet

[Download the Prioritized Approach for PCI DSS 1.2 \(pdf\)](#)

[Download the accompanying Prioritized Approach tool \(xls\)](#) including: milestones, approach summary, and attestation of compliance (requires excel 2003 or later)

Prior to completing the PCI SSC Prioritized Approach Tool, please ensure that your version of Microsoft Excel is properly configured. The option to "Extend data range formats and formulas" must be unchecked in order to return accurate results. Complete instructions are available [here](#).

To achieve PCI DSS compliance, an organization must meet all PCI DSS requirements, regardless of the order in which they are satisfied or whether the organization seeking compliance follows the PCI DSS Prioritized Approach. These documents do not modify or abridge the PCI DSS or any of its requirements, and may be changed without notice.

PCI SSC is not responsible for errors or damages of any kind resulting from the use of the information contained herein. PCI SSC makes no warranty, guarantee, or representation as to the accuracy or sufficiency of the information provided herein, and assumes no responsibility or liability regarding the use or misuse of such information.