# Best Practices
## (PDshop Security Tips)

For use with all versions of PDshop
Revised: 12/29/17

# Table of Contents

# Best Practices

## 1. Periodically check that your database is properly secured and protected against unauthorized access.

**MSSQL (SQL Server)**

If you have PDshop configured to use an SQL Server database, make sure that the SQL server is properly firewalled. Be sure to use strong passwords when creating your SQL Users.

**MSAccess (Microsoft Access)**

If you have PDshop configured to use an Access database, make sure it is impossible for someone (other than you) to download/access your database file. Your database directory should be configured with appropriate permissions (Security) so that only PDshop can read/write to the database, but no one else can see or download it. We recommend that your database be kept in a special directory that not accessible to web users. Consult with your web host or server administrator for their procedures and suggestions for securing database directories.

IMPORTANT: We strongly recommend that you rename your database file and rename the directory it is in. You should use unique names that only you would know, do not use the default names. For example, do not leave your database with a name like "pdshoppro.mdb". Don't forget to update your web.config connection string paths accordingly.

## 2. Rename your "admin" directory to help protect against unauthorized access.

The PDshop Admin is a very sensitive area because anyone with access can modify the content in your storefront, view customer information, change settings, upload files, and more. It is important to make sure that no one except you knows the directory (location/Url). We highly recommend that you rename the "admin" directory to something unique that only you would know. This will make your PDshop Admin invisible to bots and hackers. You will need to update your web.config file's "pdadminfolder" value accordingly. Do not include the new name in any robots.txt files.

## 3. Change your passwords often, and do not use the same username/password combinations more than once.

Change your passwords at regular intervals and make sure your PDshop Admin username/password is not the same as your FTP, hosting account, or server control panel logins. This can be devastating if your password is ever found or discovered thru some of the various hacking techniques. Your PDshop Admin logins, FTP logins, and hosting account/server logins should all be different. And always use strong passwords.

## 4. Make sure your web server is properly firewalled and all of its software is kept up-to-date.

A web server with inadequate firewall protection, insufficient permissions, support for weak/outdated encryption, support for outdated protocols, or with unpatched/outdated software, can make your website vulnerable to unauthorized access, hacking, malicious attacks, and malware/virus infection. See the "PCI Compliance" section of this guide for more information regarding important standards and practices.

## 5. Download and Install the latest version of PDshop periodically.

Our developers are always improving how PDshop works, for this reason revisions to each edition of PDshop are released from time to time. These revisions/updates are full versions that often contain

improvements, bug fixes, security updates, and even new features. To download the latest revision, login to your account and click 'My Downloads'. See the Installation Guides for help with installation or upgrading procedures. If you need assistance with installing these revisions/updates, contact us. NOTE: If you are using a customized version of PDshop or made your own script changes, consult with your web developer before installing any revisions.

## 6. Enable all Security Settings and Security (PCI-DSS) Features.

Since you may be hosting PDshop on a public or "shared" web server, as a general precaution, we do not recommend storing sensitive credit/debit card information in your PDshop database. If you are processing these cards, you should do so thru one of the payment gateways that PDshop supports. When processing thru the supported payment gateways, PDshop DOES NOT need to store any credit card information; it is securely passed to the payment gateway's own system for processing. Storing credit card data on your own web site can put your customer's information at higher risk. If you do choose to store or process payments, be sure to enable all PCI-DSS features and make sure you are in compliance; see the "PCI Compliance" section of this guide.

Below is a partial list of recommended features. If your version does not have these features we recommend upgrading to a version that supports these:

**Recommended Security Features**

Do Not Display Credit Card Numbers
Do Not Save Credit Card Numbers
Require Card Security Code
Enforce Transaction Limits

**Recommended Advanced Security Features**

Enforce Strong Passwords (enable in your web.config)
Enforce Strong Admin Security (enable in your web.config)
3DES Encryption (enable in your web.config)
Password Hashing (enable in your web.config)
Captcha (enable in your web.config)
Event Logging (Audit Trail) (enable in your web.config)
Web.config Encryption
Database Cleanup (Remove Credit Card Data)

## Special Notes

If your copy of PDshop was installed by a 3rd party, you may need to contact the person or company who handled your installation, or order the "Installation Service" from us.

# PCI Compliance

## *Payment Card Industry Data Security Standard (PCI DSS)*

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is done annually — by an external Qualified Security Assessor (QSA) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

## *Overview of PCI DSS Requirements*

**Build and Maintain a Secure Network**

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

**Protect Cardholder Data**

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

**Maintain a Vulnerability Management Program**

5. Use and regularly update anti-virus software on all systems commonly affected by malware
6. Develop and maintain secure systems and applications

**Implement Strong Access Control Measures**

7. Restrict access to cardholder 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

## *What am I required to do?*

If you are a merchant and you are accepting credit/debit card payments, you should contact your merchant bank/processor to determine what level of Compliance is required. Depending on the level, usually determined by the number of transactions you process, you may need to be validated by a QSA, although (for smaller businesses) you might only need to complete a Self-Assessment Questionnaire (SAQ). As far as PDshop, make sure you have enabled all of the PCI-DSS features. See the "PCI-DSS Features" section in this guide. Because PCI Compliance encompasses many aspects of security, which may be beyond the scope of PDshop, other action may be required by you. For more information, contact your merchant bank/processor or the Payment Card Industry Security Standards Council at www.pcisecuritystandards.org.

# PCI-DSS Features

## Overview

PDshop was developed to meet the PCI DSS. While most features are "behind the scenes" and require no action by you, you will need to enable the features described below during installation.

## Enabling PCI Features

### Admin Settings

The setting(s) below are found in the PDshop Administrator on the "Payment Gateways" page, under the "Settings" tab:

"Do Not Display Credit Card Numbers"

### Web.Config Settings

The settings and features below need to be enabled in your web.config file. See the "Advanced Settings" and "web.config" sections in the Installation guide for the keys required and instructions for editing your web.config.

1. Enforce Strong Passwords
2. Enforce Strong Admin Security
3. Enable 3DES Encryption
4. Password Hashing
5. Captcha
6. Event Logging (Audit Trail)
7. Web.config Encryption

## Version Notice

If you are using version 9 or earlier of PDshop, your version might not meet the most recent PCI requirements. If you are accepting or processing credit cards using PDshop with an older version, you must upgrade in order to be in compliance.

# Terms & Conditions

This guide is intended for licensed users only. All copies of the software that powers your Storefront & Admin must be properly licensed by the software vendor. Unauthorized duplication of this material, including the software or scripts that power your Storefront & Admin, is strictly prohibited. Contact your web master or systems administrator for more information.