

Security Checklist for users of PDG Commerce and PDG Shopping Cart

While PDG Software has designed this document to contain a list of items that should be verified when using PDG Commerce and PDG Shopping Cart, it should not be considered comprehensive. Web security requires constant communication between you, your server administrator, and the provider of any software applications utilized on your web server. **PDG Software, Inc. does not guarantee this list will make any site absolutely secure.** This checklist is not intended to provide a complete security check for your site, though it is an excellent starting point.

Each of the items below should be confirmed with your site administrator, server administrator, and any other party(s) necessary. If you are unsure of the appropriate party to contact for each portion of the checklist, please contact PDG Technical Support at <http://support.pdgsoft.com> for assistance.

- ❑ PDG Software updates – Verify that PDG Commerce or PDG Shopping Cart has been upgraded to the most recent version available. The most recent versions of PDG Commerce and PDG Shopping Cart include a considerable number of security features including IP tracking, IP blocking, automatic encryption of user name and password data for the Merchant Administrator and payment services, session based administration, and much more to help protect you and your web store.
- ❑ Operating system updates – Verify that all operating system patches and upgrades have been installed to the server where your site resides. Failure to do so can result in the compromise of your entire web server.
- ❑ Web server updates – Verify that all web server software programs (including web server, SSL modules, etc.) have the appropriate patches and upgrades in place.
- ❑ Windows permission, IIS, and Web Service Extensions settings – For Windows NT/2000/2003 users, confirm that IIS, file permissions, and web service extensions (Windows 2003 only) have been set per the PDG Software documentation found at <http://www.pdgsoft.com/security.htm>.
- ❑ UNIX .htaccess protection – For UNIX users, confirm that you have the appropriate .htaccess file located within your PDG_Commerce or PDG_Cart directory. Additional information regarding .htaccess can be found at http://www.pdgsoft.com/unix_security.htm.
- ❑ Placement of PDG directory and order log files – The latest versions of PDG Commerce and PDG Shopping Cart allow users to choose from a number of locations to store their PDG_Commerce or PDG_Cart directory, including the option of storing it outside of the site's document root directory so that it is unavailable via URL queries. The three locations that PDG Software will attempt to locate the PDG_Commerce or PDG_Cart directory are one directory above the document root,

within the document root, or within the cgi directory in which the PDG Commerce or PDG Shopping Cart executables are stored.

Note: It is not required that your order log files be created and stored within the PDG_Commerce or PDG_Cart directory. You may supply a full server path to a protected directory, or you may use “../” to specify a path relative to the PDG_Commerce or PDG_Cart directory.

- ❑ Do not log credit card data – Within the “Commerce Options” or “Cart Options” section of your web site’s PDG Merchant Administrator, users may elect to have credit card data omitted from their order log files and email notifications. All merchants utilizing an online payment gateway should take advantage of this ability as transaction data may be retrieved from the gateway by referencing the invoice number for a particular order.
- ❑ GPG encryption – If you have elected to enable order logging and/or vendor email notifications that may contain sensitive data, PDG strongly encourages you to take advantage of PDG Software’s compatibility with GnuPrivacy Guard (GPG). GPG offers 128-bit encryption for sending and storing sensitive data. Documentation for implementing GPG encryption can be found at <http://www.pdgsoft.com/docs/Encryption.pdf>.
- ❑ SSL (Secure Socket Layer) web certificates – SSL certificates issued by PDG partners such as VeriSign, Thawte, and GeoTrust encrypt all data as it is in transit from a customer’s web browser to your web server. Please see your PDG Commerce or PDG Shopping Cart User Guide for instructions for adding SSL to your PDG Software program.
- ❑ Passwords – All passwords, including your PDG Merchant Administrator password, password for online payment services, and FTP/web access accounts should contain a minimum of eight characters and include a combination of alpha and numeric characters. Avoid using common names, birth dates, children’s names, site names, etc. as passwords or user names. Passwords should also be changed on a periodic/frequent basis. Do not use the same password for all accounts (e.g., FTP, payment service, Merchant Administrator, etc.).
- ❑ File naming – Similar to choosing a password, merchants should also use caution when determining the names of order log and payment gateway log files. **Default file names should never be used for order log files.** Select a file name that cannot be easily guessed and would not be apparent to an unauthorized user.
- ❑ Authorized users – Verify that only authorized users have access to your web site and PDG Merchant Administrator. Do not share your passwords with any unauthorized individuals. Verify that all former employee access is terminated immediately after employment has ended and that any site passwords they may have had access to are

changed. If it is necessary to provide your account information to a third party, be sure to change the password as soon as the situation is resolved.

- ❑ Archiving previous orders – Download and remove order log files from your web server on a regular basis. PDG Software will automatically create new log files with the same names on the next order any time you download and delete your order log files.
- ❑ Payment gateway setup – If you are utilizing an online payment gateway to accept credit cards or checks online, be sure that you adhere to the setup process referenced in the PDG Commerce or PDG Shopping Cart User Guide and your payment service provider’s instructions.
- ❑ Disposal of printed materials – Be sure to dispose of any printed order log files and email notifications in the appropriate manner (e.g., shredding).
- ❑ Removing welcome page – The commerce.html or cart.html page located in the document root directory of your web is for familiarizing yourself with PDG Commerce or PDG Shopping Cart. This file should be removed, renamed, or relocated as you acquaint yourself with PDG Software to make it more difficult for a malicious web user to determine which software is being utilized on your web site.
- ❑ Renaming executables – The “commerce” or “shopper” executable file in use on your site may be renamed to any name (based on your server configuration, it may be necessary to maintain the “.exe” or “.cgi” file extension) to make it more difficult for a malicious web user to identify the software being utilized on your web site. It is important that your web pages reflect the new name or your customers will encounter “file not found” errors when attempting to purchase items on your web site.

Note: When upgrading to new minor version patches of the PDG Commerce or PDG Shopping Cart program, you will need to rename the “commerce” or “shopper” executable file in the upgrade to the name you are using on your web site.

- ❑ Firewall – Install and maintain a working network firewall to protect sensitive data that is available via the Internet.
- ❑ Web access logs – Verify with your server administrator that access logs are being created for all queries to your web site. In the unfortunate event that the server or your site is compromised and an unauthorized user gains access, these files will assist in determining how the user was able to bypass your security settings.