

Implementation security guidelines

After the program started for the first time you must take the following steps in order to be PCI compliant.

1. At the login screen, click on "Change Password". Assign a good (complicated) password to the "admin" that is hard to guess. Look for PA-DSS documentation on password guidelines. PA-DSS document is available upon request from us or from all approved assessors.
2. Click on Setup, Click on Global Setup, click on "Encryption Password" and click "Add". Fill in the grid on the left on the "EncryptionPassword" row a complicated password to be used by your business.
3. Do not use the "Admin" account for any tasks used to run the business (such as creating new items, making sales etc.)
4. Click on Utilities, Security and press on the "create Levels" button. That creates 2 templates for Cashier and a manager.
5. Create your own account, give yourself a name, a good password and assign for yourself an "admin" level.
6. Create your users and assign to each user either a manager (MGR) or a cashier (CASH) level.
7. In the security module search for the user "CASH" and go over the allowed tasks. A task that is not needed should be changed to "not allowed". Pay special attention to the transactions involving credit cards and credit card reports.
8. Create a new SQL user account that is restricted to use only the VRP database and the TempDB.
9. Change the file VRP.INI to match you VRP store ID and Register number along the login name and password used for SQL create in the previous step.
10. Ensure that your router does not forward a public IP to the SQL server. Only VPN IP's can access the SQL server.
11. Make a plan to purge credit card data on a regular interval. Delete all card data that is not needed for running your business. The purge card data program can be accessed from the utilities menu. We recommend to add to the scheduler a daily task to delete card data older than required for running your business.