QuickBooks Point of Sale PCI Compliance Recommendations

- The workstation(s) that QuickBooks Point of Sale is running on should not be used for any internet access (email, web browsing, streaming music, etc.) unless it directly relates to operating QuickBooks Point of Sale.
- There should not be any other workstations attached to the same network segment that QuickBooks Point of Sale is running on. Any other network devices must be on a separate network segment that has no access to any of the devices on the network segment that is strictly used for QuickBooks Point of Sale.
- There should not be any devices (tablets, smartphones, laptops, workstations) connected to the same network segment via a wireless connection (WiFi) that the QuickBooks Point of Sale workstation(s) are running on. Any normal wireless network (not guest wireless network) should be disabled completely or properly segmented so that it has no access (inbound or outbound) to any other network segment.
- Any devices that need wireless connectivity MUST either be contained to a guest wireless network or properly segmented wireless network that has no communication with the physical wired network segment that QuickBooks Point of Sale is running on. This is to ensure that the guest network/properly segmented wireless network is sandboxed and not able to communicate in any way, shape, or form with the wired network that QuickBooks Point of Sale workstations are running on and vice versa. WEP should not be used as an encryption method for any wireless network.
- All vendor supplied accounts and passwords for all devices used on the network (switches, routers, etc.) should be changed from their defaults and properly documented for future use. All vendor accounts should be disabled until their use is specifically required.
- At least two separate Windows users should be created on every workstation that runs QuickBooks Point of Sale. The first user in Windows would be strictly for running QuickBooks Point of Sale and would be configured as a normal Windows user. The second user in Windows would be a user that would only be used when administrator privileges are required (for example:installing Windows Updates, updates to QuickBooks Point of Sale, installing device drivers, etc.) This is to make sure that the user in Windows that is running QuickBooks Point of Sale has the least amount of security rights as possible to operate QuickBooks Point of Sale and to further prevent unintended infection from malicious sources. The best case scenario is that every employee that will use QuickBooks Point of Sale needs to have their own user account in Windows. By having individual user accounts in Windows for all employees who use QuickBooks Point of Sale, it is easier to track employee usage of the software for auditing purposes.
- All workstations running QuickBooks Point of Sale should have both antivirus and firewall software installed/configured from a reputable software developer to help protect and prevent the infection of the workstations by malicious sources. Both applications should be updated daily and have full virus scans run every day. The logs for the antivirus scans should be reviewed every day to make sure that nothing was infected.
- QuickBooks Point of Sale should be configured to require the software to be logged into and not allow unauthenticated access to it.
- Every employee who uses QuickBooks Point of Sale needs to have their own user account in QuickBooks Point of Sale that they use to log into and use the software. By having individual user accounts in QuickBooks Point of Sale for all employees, it is easier to track employee usage of the software for auditing purposes.
- Only give the users in QuickBooks Point of Sale the least amount of security rights as they need to perform their job duties. This will prevent employees from accessing other areas of the application that they do not need to. QuickBooks Point of Sale has 4 predefined security groups that can be modified or copied. You have the ability to create your own security groups either from scratch or from an existing security group.

QuickBooks Point of Sale PCI Compliance Recommendations

- Create a security group in QuickBooks Point of Sale that has no rights to the application. When an employee leaves, reassign their user account in QuickBooks Point of Sale to the security group with no rights. This will allow you to keep their user account for auditing purposes, but not allow the user to have any rights to using the software at all.
- Configure QuickBooks Point of Sale at a workstation level to automatically log users out after a specific period of inactivity (ie:5 minutes). This will help prevent unauthorized access to the application.
- Configure QuickBooks Point of Sale to log the user out of the software after every sale has been completed. This will help prevent unauthorized access to the application.
- Configure the screen saver in Windows to lock the screen after a period of inactivity after a couple of minutes. Also require that the user provide their credentials to unlock the screen saver. This will also help prevent unauthorized access to both the workstation first and to the application second.
- Configure the workstation(s) to require users to change their operating system password every 90 days.
- Configure the workstation(s) to require that the operating system passwords meet certain requirements for the passwords to be used (minimum 7 characters including upper case, lower case, numbers, and special characters).
- Configure the workstation to remember the last four passwords used so that an employee is not able to reuse the same password over and over again.
- Require that your users change their passwords in QuickBooks Point of Sale every 90 days. Passwords for QuickBooks Point of Sale may be up to 20 characters long and include upper case letters, lower case letters, numbers, and special characters).
- It is highly recommended that any passwords used do not contain any of the following pieces of information:
    - Name
    - Nickname
    - Username
    - Kids names, birthdates, or any other types of personally identifiable pieces of information.
- If you suspect a security breach by a specific user/employee, you should either disable their account(s), change the password for their account(s), or delete their accounts. This will block further access to your data by the user/employee while you have an opportunity to investigate the suspected breach.
- When an employee leaves your company, disable their account immediately by deleting the employee record so that no further access to your data through that user name and password is possible (if you wish to keep the employee record, change their password and reassign them to a security group with no rights).
- Make sure that every workstation is configured to install Windows Updates as soon as they are available. Once the updates have been installed, it is necessary to reboot the workstation to make sure that the updates have taken effect. Check the Windows Updates history to make sure that they are being installed without error. Windows Updates are released on the second and fourth Tuesdays of each month. The second Tuesday is referred as “Patch Tuesday”.