PCI Compliance

Is TallySoft PCI Compliant?

YES, all platforms used to process credit cards with TallySales are PCI Compliant.

What is PCI Compliance?

PCI Compliance is a set of security and procedural requirements for all merchants who process, store or transmit payment cards in their business, including credit and debit cards, gift cards, and pre-paid cards. Being compliant means that your business adhered to the *Payment Card Industry Data Security Standard* (PCI DSS) requirements for security management, policies, procedures, network architecture, software design and other critical protective measures." It is an ongoing process that should be part of your everyday operations. It means that "you are playing your role to make sure that your customers' payment card data is being kept safe throughout every transaction." (PCI-DSS Version 3.0)

Why is it Needed?

The basic reason is to reduce fraud.

Who Created It and why?

It was created in 2006 by The PCI Security Standards Council, an organization made up of representatives from the major card brands: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

Prior to 2006, each card brand had individual requirements for processing payment cards. Merchants were required to adhere to the requirements for each card brand they accepted. Complying was difficult for merchants, as many of the requirements were overlapping but had minor variations. To ensure a more consistent and secure environment, the card brands worked together to form an industry standard resulting in the PCI DSS in November 2008. Beginning in 2010, the requirements are updated every three years. The most recent update, PCI DSS Version 3.0, was released in November 2013.

Who requires it?

As a merchant who accepts payment cards, you must meet PCI Data Security Standards requirements set by the PCI DSS Council. By signing a merchant services contract, you have agreed to maintain compliance.

What is the PCI Data Security Standard?

The Payment Card Industry Data Security Standard is comprised of twelve technical and operational standards that must be continuously maintained by all organizations and merchants, regardless of their size or the number of transactions they process. If your business accepts credit cards, you must comply with the PCI DSS.

The PCI Data Security Standard is made up of 6 major goals:

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

What happens if I'm not compliant?

If you are at fault for a security breach, you can incur fines and penalties from the major card brands, legal costs, the cost of reissuing new payment cards, and lose the ability to accept payment cards.

What are the details?

Within the six goals set in the PCI-DSS are twelve requirements, each one consisting of up to ten components, and many more sub-components. The twelve requirements are stated below along with a brief summary.

1. Install and maintain a firewall configuration to protect cardholder data.

   Every merchant needs to work with your IT department or consultant to configure your network to protect the cardholder data environment from unauthorized access. Maintain a network diagram and written policies for configuring and maintaining your environment.

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

   In addition to TallySales passwords, you should create individual passwords for all software, network devices, and wireless networking; and disable unnecessary accounts after installation.

3. Protect stored cardholder data.

   You must minimize storage of cardholder and sensitive authentication data. Ensure the Personal Account Information, (PAN), is unreadable after the transaction is processed. Create security policies and operational procedures to protect cardholder data and ensure that all required parties are advised.

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

   Implement security controls to safeguard cardholder data during transmission over open, public networks such as the Internet, wireless technologies, cellular technologies, GPRS and satellite communications. Never send unprotected PANs via e-mail, instant messaging, chat, etc. Ensure that all affected parties are provided with documented policies and procedures for managing secure transmission of cardholder data on an ongoing basis.

5. Protect all systems against malware and regularly update anti-virus software or programs.

Deploy and maintain anti-virus and anti-malware software on all systems: personal computers, tablets, and servers. Ensure that all mechanisms are actively running and cannot be disabled or altered except by authorized users and only for a limited amount of time. Provide all applicable parties with documented policies and procedures.

6. Develop and maintain secure systems and applications.

   All systems must have up to date software patches to protect against the exploitation and compromise of cardholder data. Create a method for determining vulnerabilities on an ongoing basis. Provide all applicable parties with documented policies and procedures.

7. Restrict access to cardholder data by "business need to know".

   Ensure that all critical data can only be accessed by authorized personnel on a need to know basis. Grant access according to job roles and limit access to only those with a legitimate business reason. Restrict access to all other users. Provide all applicable parties with documented policies and procedures.

8. Identify and authenticate access to system components.

   To ensure accountability within your cardholder environment, create user IDs for all employees, vendors and other third-parties; do not use one ID for several employees. Maintain user lists by deleting terminated users immediately, and deleting inactive users every 90 days. Enforce lock-out restrictions and strong password policies. Grant remote access to in-house and third parties on a limited basis. Provide all applicable parties with documented policies and procedures.

9. Restrict physical access to cardholder data.

   Restrict malicious access to cardholder data environment. Keep cardholder data, backups and reports in secure locations and shred hard copies containing payment information when they are no longer needed. Implement policies limiting physical access to sensitive areas where cardholder data can be obtained, such as computers and servers, publicly accessible network jacks, wireless access points, handheld devices, networking/communications hardware, etc. Protect all devices that capture payment card data from tampering and substitution, and maintain an up to date list of all devices. Provide all applicable parties with documented policies and procedures.

10. Track and monitor all access to network resources and cardholder data.

    Review audit logs from TallySales and your credit card gateway provider on a daily basis to prevent, detect or minimize the impact of a data compromise. Provide all applicable parties with documented policies and procedures.

11. Regularly test security systems and processes.

    Implement a process for detecting the presence of unauthorized wireless access points and be able to identify both authorized and unauthorized access points on a quarterly basis. Run internal and external vulnerability scans on a quarterly basis, or as required by your Approved Scanning Vendor. Provide all applicable parties with documented policies and procedures.

12. Maintain a policy that addresses information security for all personnel.

    Create and disseminate a strong security policy that informs users what is expected of them. Users should be made aware of the sensitivity of this data and their responsibilities for protecting it. This includes all employees, contractors and consultants who are on site and

those who have remote access to your cardholder environment. Provide all applicable parties with documented policies and procedures.

The above information is believed to be correct, however, TallySoft is not to be held liable for any errors, or any damages resulting from errors. This information is for the sole purpose of educating business owners. All recipients of this form are encouraged to do their own additional research or consult with an attorney prior to implementation of any actions that may fringe upon PCI compliance procedures.

RESOURCES PCI Security Standards at https://www.pcisecuritystandards.org/