

What is **PCI** **Compliance?**

PCI Compliance is the Payment Card Industry Data Security Standard, **a world-wide benchmark** mandated by the card brands, Visa, MasterCard, American Express, Discover and JCB **for the protection of cardholder identity and transaction information.** The PCI standard asks merchants and service providers to meet minimum standards of security when storing, processing and transmitting this customer data. This is also *known as PCI compliance.* All merchants, regardless of transaction volume or processing method are required to adhere to the PCI standards.

Over the next few months, we will be sharing information with you on how we can help you become compliant and avoid potential data breaches. You may visit the PCICO website <https://www.pcisecuritystandards.org/> for further information. On the back of this notice, we have provided you with the "Dirty Dozen" elements that serve as the foundation for PCI compliance and should be used in the day to day operation of your business.

The Dirty Dozen PCI Data Security Standard

Build and Maintain a Secure Network

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

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to 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