



Transaction Network Services

What are the Payment Card Industry Data Security Standards?

PCI DSS consists of a standardised, industry-wide set of requirements and processes.

Its purpose is to ensure that valuable cardholder account data is always secure.

It comprises 12 key requirements.

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for passwords or other security parameters
3. Protect stored data
4. Encrypt the transmission of cardholder data and sensitive information
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
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
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

By implementing PCI DSS, your business will automatically comply with the requirements and regulations set out by international card payment schemes and acquiring banks.

Full details can be accessed at

www.visaeurope.com/aboutvisa/services/security/accountinformationsecurity.