

## Data protection: PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) exists to reduce credit card fraud. It is a set of twelve security standards that any organisation which stores, processes or transmits payment card data in an electronic or paper system needs to meet. These standards are set by the major payment card brands to make sure serious steps are taken to protect payment card data.

### How to be, and stay, compliant

All organisations which process, store, or transmit credit card data, i.e. in online or telephone donations, purchases or bookings, need to comply with the standards. This process involves: **Assess**, identify cardholder data/processes and analyse vulnerabilities; **Remediate**, fix vulnerabilities; and **Report**, Report compliance and present evidence that controls are in place.

There are four different levels of compliance, dependent on the annual number of credit card transactions. Levels 1-3 apply to organisations which process 20,000 or more transactions a year; these organisations will/may require a third party auditor. The **majority of not for profit organisations will be in Level 4**. Level 4 organisations process fewer than 20,000 a year and can carry out a **self-assessment** questionnaire. The exact compliance requirements will differ between payment brands. Use the PCI Security Standard guidance to [get started](#).

The PCI Security Standards Council provides general guidance: (1) Sensitive Authentication Data should never be stored, (2) If you don't need cardholder data, don't store it, and (3) If you do need cardholder data, isolate and protect it.

### Questions to ask

- Are documents kept for audit purposes secured?
- Are donations, e-commerce and third party providers compliant?
- Have default settings and passwords been changed?
- Are monitoring systems in place - are all security patches up to date?
- Is there an information security policy?

If cardholder data is stolen, as well as a **fine** and the risk of **loss of right to accept payment cards**, there is a **significant risk to reputation**.

### 12 security standards for payment card data

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder 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 Information Security Policy	12. Maintain a policy that addresses information security

### Further information

PCI Security Standards Council: [Quick reference](#) | [How to be compliant](#) | [Guide for merchants](#)  
Sayer Vincent Guides: [Information security management made simple](#) | [Data Encryption](#) | [Digital Certificates](#)