

The International Card Payment Schemes introduce a new global security standard:

PCI DSS

Data compromise, and using card data to commit fraud is a worldwide concern to all parties concerned. Security within the global card payment system is therefore something which affects us all – banks, merchants, and not least cardholders. As a result, Visa and MasterCard have worked together to draw up a common global standard for secure card data management: PCI DSS.

PCI DSS is a global standard, which all the major international card schemes have signed up to. The aim of PCI DSS is to enhance card data security. It involves minimising the risk of computer hacking, and the theft and misuse of card data, while also upholding and boosting the confidence in using cards as a method of payment.

PCI DSS affects us all

All merchants, acquirers and other parties who process, store or transfer card data must adhere to PCI DSS. The general requirements can be summarised as follows:

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 within the business on a need-to-know basis
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

More information will follow

As a Euroline merchant, you will be kept up to date with advice and information relating to PCI DSS. You can start by mapping the flow and processing of card data within your organisation. Remember always to store card data and receipts securely, to keep your terminal secure and to change your terminal PIN code regularly. Don't forget that only authorised persons may carry out card transaction refunds, since the sum refunded is always charged to your company's bank account. And remember to ensure that staff training on secure card handling is kept up to date.

Further details

The latest information and FAQs can be found at www.euroline.se
www.visaeurope.com/aboutvisa/security/ais/aisprogramme.jsp
sdp.mastercardintl.com
www.pcisecuritystandards.org/

PCI DSS: the advantages for your company

As a merchant, implementing PCI DSS means that you meet the mandatory requirements which all major card schemes now place on all those who use the international payment system. This brings many benefits.

- Greater knowledge and security awareness within your business.
- Your business is protected against unauthorised access to its systems and processes.
- Your business is protected against the risk of suffering major financial losses.
- You minimise the risk of negative publicity and damage to your brand.
- Enhanced security can help boost customer confidence – and possibly also increase sales.