



Make sure you fulfil the PCI DSS requirements to reduce risks

- both for yourself and your customers!

Checklist

Mandatory requirements concerning handling of card information.

PC DSS is an extensive set of rules and regulations to ensure that card information is always handled in a secure manner. Many of the requirements relate to the IT environment, but stringent requirements are also placed on merchants' processing in everyday operations. It concerns how you handle receipt copies, electronic media, passwords to point-of-sale terminals, authorisation to personnel, etc. Below is a compilation of some of the most important fundamental PCI DSS requirements that Visa and MasterCard have currently defined and that your company has agreed to fulfil in its acquiring agreement with Euroline.

Test security of your operations.

If you cannot answer YES to all questions, there are deficiencies that you should correct as soon as possible. You always have sole responsibility for handling card data in your operations, both in regard to physically and digitally stored information.

1. Documents with card numbers and media used in handling card information.	Yes	No
--	------------	-----------

Do you store all paper and electronic media with card information in a secure manner (under lock and key, for example), where they can only be accessed by authorised persons? (Such media includes computers, electronic media, network and communications hardware, telecom lines, paper receipts, paper reports and faxes.)	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------

Do you maintain strict control over storage of and access to media that contain card information?	<input type="checkbox"/>	<input type="checkbox"/>
---	--------------------------	--------------------------

Do you destroy card information stored on media when it is no longer needed for your operations?	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------

2. Internal routines and policies.

Have all personnel who work with accounting and administration, including cashier staff, received information about the responsibility they have for card information and the routines that apply?	<input type="checkbox"/>	<input type="checkbox"/>
--	--------------------------	--------------------------

Is access to computer equipment and card information limited to persons whose job duties require such access?	<input type="checkbox"/>	<input type="checkbox"/>
---	--------------------------	--------------------------

Do security policies and routines clearly and plainly specify the responsibilities of employees, suppliers and contractors in regard to information security?	<input type="checkbox"/>	<input type="checkbox"/>
---	--------------------------	--------------------------

Have you established incident plans and escalation routines, and arranged support for them in operations so as to ensure effective and appropriate handling in all situations that may occur? **Ja Nej**

Is there a formal security training programme for instructing all employees of the importance of data security when handling cards and card information?

3. External suppliers.

Are the following requirements included when your company signs agreements with service suppliers that have access to the company's card information?

- That the supplier of the service complies with the industry's data security standard PCI DSS?
- That the supplier is responsible for security relating to card information stored by the supplier?

4. Supervision of your point-of-sale terminal.

Is the payment terminal located so that you can take responsibility for it not being manipulated by unauthorised persons?

Does the company have routines for handling the payment terminal's passwords, which entail that:

- Only authorized personnel have access to passwords?
- Passwords are stored securely?
- All personnel with access to a password have received training and instructions that they are not to disclose it to anyone?
- Passwords are regularly changed and that a password that you suspect of having been released to an unauthorised person is immediately changed?

Do you ensure that the contents of your company's technical equipment do not become accessible to an unauthorised person in conjunction with service?

Do you ensure that no card numbers are stored in your technical equipment upon scrapping or sale?

Do you ensure that technical service via external logins is only carried out after you have approved the connection, and that logouts are conducted after service is completed?

Continued on next page

Please contact us if you would like help or advice.

If you would like help with the test or advice about how you can best adapt your operations to the requirements of PCI DSS, please contact Euroline's Customer Support at +46 (0)8 14 69 30 or via e-mail: euroline@seb.se

cont.

5. Handling of data for authentication and authorisation.

Yes No

Do all of your company's systems comply with the following requirements concerning storage of sensitive data for authentication?

- Do you ensure that no authorisation data that you obtain from the card's magnetic track, chip or other location is stored?

(To minimize risks, you may only store the data elements that are necessary for operations. It is normally enough to store: The accountholder's name, card number, expiration date and service code.)

- Are you sure that authorisation data is never stored after completed authorisation, not even in logs? (This applies to encrypted information.)

- Can you guarantee that you do not store the security code CVV2/CVC2, which is used to verify transactions when a card is not present during a transaction (card-not-present)?

- Do you ensure that you do not store personal identification numbers (PIN) or encrypted PIN blocks?

- Are there policies, procedures and routines for preventing non-encrypted card numbers from being sent via e-mail?

PCI DSS

To further raise the level of security in global payment systems, the card industry has agreed to a global common security standard. The standard is called the Payment Card Industry Data Security Standard (PCI DSS) and embraces all card networks. This entails that all merchants, acquirers and other parties that transfer, process or handle card information must comply with the requirements of PCI DSS, so as to safeguard international payment systems. Failure to fulfil the requirements involves significant financial risks and could result in forfeiture of your right to accept card payments.

EUROLINE[®]

