

## **PCI-DSS = Payment Card Industry Data Security Standard**

PCI-DSS is a security standard based on strict guidelines designed to ensure accurate and secure handling of credit card data. This standard was introduced by major credit card companies such as Visa, MasterCard, American Express and JCB.

In order to protect sensitive (financial) data of merchant partners and participating cardholders, it is required that cardholder data processed by merchants be shielded against hacker attacks.

### **The requirements contained in PCI-DSS are as follows:**

1. The set-up and maintenance of a firewall designed to protect cardholder data
2. The modification of default passwords/security parameters supplied by (software) vendors
3. Protection of stored cardholder data
4. Encrypted transmission of cardholder data across all open and/or public networks
5. Use and regular updating of anti-virus software solutions
6. Development and use of secure systems and applications
7. Restricted access to credit card data based on a “need-to-know” basis and in accordance with job responsibilities
8. Assignment of a unique user identification code to each person with access to the computer system
9. Restricted physical access to cardholder data
10. Tracking and monitoring of all access to network resources and cardholder data
11. Regular inspections of security systems and security-related processes
12. Introduction of corporate guidelines addressing information security for company employees and contractual partners.

**This standard is binding for all corporate entities which store, process or transmit credit or debit card data.**

For further details, please visit this website <https://www.pcisecuritystandards.org/>

By following these binding PCI-DSS rules and regulations you help to ensure that both your clients and your own business will be protected against criminal attacks. This essential security will be highly appreciated by your clients.

### **The advantages for your company at a glance:**

- ✓ Your clients benefit from substantially improved data security and protection
- ✓ Enhanced customer confidence
- ✓ Protection of your corporate image
- ✓ Minimization of potential corporate risks through protection of sensitive data
- ✓ Protection against (financial) damage and possible liability claims for damages resulting from security breaches.

We encourage you to contact us in case you have any queries regarding this matter!