# How Safetica helps to comply with PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) is a standard developed to protect sensitive data concerning payment cards and data created by using such cards.

The standard itself consists of twelve requirements which are further divided into sections. To achieve a full compliance with the PCI-DSS, a company has to fulfill all the requirements stated in these sections.

Safetica can easily help you fulfill following requirements:

| The requirements of PCI-DSS | How Safetica helps |
|---|---|
| **3. Protect stored cardholder data** | |
| 3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization. | Safetica DLP > Data categories, DLP Rules |
| 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs). | Safetica > BitLocker disks |
| **4. Encrypt transmission of cardholder data across open, public networks** | |
| 4.1 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:<br>- Only trusted keys and certificates are accepted.<br>- The protocol in use only supports secure versions or configurations.<br>- The encryption strength is appropriate for the encryption methodology in use. | Safetica DLP > Channel control, DLP Rules |
| 4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.). | Safetica DLP > Channel control |
| **7. Restrict access to cardholder data by business need to know** | |
| 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. | Safetica DLP > DLP rules, Disk Guard |
| 7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. | Safetica Supervisor > Application control, Web control<br>Safetica DLP > DLP rules, Device control, Channel control |
| 7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties. | Safetica DLP > DLP protocol |

| | |
|---|---|
| **9. Restrict physical access to cardholder data** | |
| 9.7 Maintain strict control over the storage and accessibility of media. | Safetica DLP > Device control |
| **10. Track and monitor all access to network resources and cardholder data** | |
| 10.1 Implement audit trails to link all access to system components to each individual user. | Safetica settings and logs |
| 10.2.1 All individual user accesses to cardholder data | Safetica Auditor > Files<br>Safetica DLP > DLP rules, DLP protocol |
| 10.2.2 All actions taken by any individual with root or administrative privileges | |
| 10.2.7 Creation and deletion of system level objects | |
| 10.3 Record at least the following audit trail entries for all system components for each event. | Safetica logs |
| 10.5 Secure audit trails so they cannot be altered. | Management and settings > Access Management |
| 10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. | Safetica logs, Alerts, Reports |
| 10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). | Safetica > Maintenance > Database management |
| **11. Regularly test security systems and processes.** | |
| 11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. | Safetica Auditor > Files |
| **12. Maintain a policy that addresses information security for all personnel.** | |
| 12.3 Develop usage policies for critical technologies and define proper use of these technologies. | Wide range of Safetica tools. The most important ones:<br>Safetica Auditor > Files, Web sites, E-mails, Applications, Print |
| 12.3.1 Explicit approval by authorized parties | |
| 12.3.2 Authentication for use of the technology | |
| 12.3.3 A list of all such devices and personnel with access | |
| 12.3.5 Acceptable uses of the technology | |
| 12.3.7 List of company-approved products | Safetica Supervisor > Application control, Web control, Print control<br>Safetica DLP > Disk Guard, Device control, DLP rules, DLP protocol |
| 12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures. | Safetica > Notification |

17-1018

Safetica Technologies s.r.o., Laubova 1729/8, 130 00 Prague 3, Czech Republic, www.safetica.com