



PCI Compliance and the Data Security Standards

For more information visit www.axiapayments.com/pci

Axia 
Your partner in payment services

Introduction



The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

For more information visit www.axiapayments.com/pci



Introduction, cont'd



The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.

Ongoing development of the standard will provide for feedback from the Advisory Board and other participating organizations. All key stakeholders are encouraged to provide input, during the creation and review of proposed additions or modifications to the PCI DSS.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

For more information visit www.axiapayments.com/pci



Secure Network Requirements



- **Build and Maintain a Secure Network**

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

For more information visit www.axiapayments.com/pci

Cardholder Data Requirements



- **Build and Maintain a Secure Network**

Requirement 3: Protect stored cardholder data. Only store data if it is absolutely necessary. We highly recommend that any card holder data for recurring transactions or customer database be stored at a compliant third party gateway.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

For more information visit www.axiapayments.com/pci

Vulnerability Management Requirements



- **Maintain a Vulnerability Management Program**

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

For more information visit www.axiapayments.com/pci

Access Control Requirements



- **Implement Strong Access Control Measures**

Requirement 7: Restrict access to cardholder data by business need-to-know. Any employee with access to cardholder data should complete a thorough background screening.

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

For more information visit www.axiapayments.com/pci

Monitoring & Testing Requirements



- **Regularly Monitor and Test Networks**

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

For more information visit www.axiapayments.com/pci

Information Security Policy Requirements



- **Maintain an Information Security Policy**

Requirement 12: Maintain an ongoing policy that addresses information security. Please visit www.axiapayments.com/pci or the PCI Security Standards website periodically in order to remain up to date on the latest information on staying compliant.

For more information visit www.axiapayments.com/pci