PCI DSS Security Standard
(Payment Card Industry Data Security Standards)

Objectives	PCI DSS Requirements
Install and maintain secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Prevent the use vendor-supplied default passwords and other security settings
Protection of cardholder data	3. Protection of stored cardholder data 4. Encryption of transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain an information security policy

For more information, please refer to the following links:

PCI SSC:
Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards

VISA:
Payment Card Industry Compliance I PCI DSS Compliance I Visa (Visa Europe - UK)

MasterCard:
PCI DSS Merchant Compliance Levels I Secure Customer Data (mastercard.us)

American Express:
PCI Compliance and Data Security | American Express[9]

Union Pay:
PCI payment gateway solution | UniPay Gateway

Diners Club & Discover Global Network:
Cards, Benefits, Airport Lounges | Diners Club International
PCI DSS Compliance Assessment | Discover Global Network