PCI DSS

Build and Maintain a Secure Network
1. Install and maintain a working firewall to protect data
2. Do not use vendor-supplied defaults for passwords and other security parameters

Protect Cardholder Data
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across 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

Technical security
Firewalls
Compartments
HTTPS
Encryption
Anti-virus

Implement Strong Access Control Measures
7. Restrict access to cardholder data by business need-to-know
8. Assign unique ID to each person with computer access
9. Restrict physical access to cardholder data

Access control
Role based access
Authentication

Regularly Monitor and Test Networks
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Ensure
Logs
Test

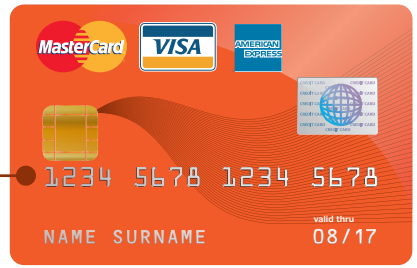
Maintain an Information Security Policy
12. Maintain a policy that addresses information security for employees and contractors

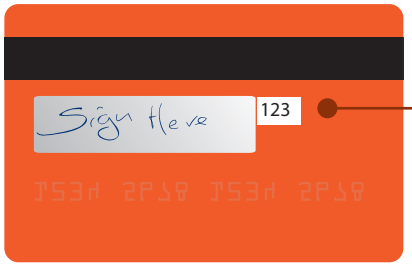
Policy
Awareness Staff

PCI DSS
The Payment Card Industry (PCI) is a council representing credit card brands like American Express, Master Card and Visa.
The council issued Data Security Standards (DSS) for organizations that process credit cards.

Risks
Reputational damage
Penalties for all cards potentially at risk
Liability for breached cards

Governance
COBIT
ITIL v3
ISO /IEC 27xxx
ISO /IEC 20000
PCI DSS





Primary Account Number (PAN)
Only store very very secured

Card Verification Code (CVC)
Don't store this

Primary Identification Number (PIN)
Don't store this