PCI Compliance Checklist

Checklist · 22 items · 8 sections

Any business that accepts credit card payments must comply with PCI DSS (Payment Card Industry Data Security Standard). This checklist covers the 12 core PCI DSS requirements in plain language so you can assess and improve your compliance posture.

Open the editable, AI-powered version online:
https://genechecklist.com/checklist/pci-compliance-checklist

NETWORK SECURITY

- [ ] Install and maintain a network firewall to protect cardholder data
  HIGH
- [ ] Change all default passwords on routers, firewalls, and payment systems
  HIGH
  Default vendor passwords are publicly known: changing them is PCI Requirement 2
- [ ] Remove or update all vendor-supplied default security settings
  HIGH

CARDHOLDER DATA PROTECTION

- [ ] Do not store full card numbers, CVV codes, or PINs after authorization
  HIGH
- [ ] Mask Primary Account Numbers (PAN) when displayed: show only last 4 digits
  HIGH
- [ ] Encrypt cardholder data transmitted over public networks using TLS 1.2+
  HIGH

VULNERABILITY MANAGEMENT

- [ ] Use and update anti-virus software on all systems that handle card data
  HIGH
- [ ] Keep payment software and systems patched and up to date
  HIGH
- [ ] Develop and maintain secure systems: follow secure coding practices
  HIGH

ACCESS CONTROL

- [ ] Restrict access to cardholder data on a need-to-know basis only
  HIGH
- [ ] Assign a unique user ID to each person with access to payment systems
  HIGH
- [ ] Restrict physical access to payment systems and printed card data
  HIGH
- [ ] Implement multi-factor authentication (MFA) for all remote access
  HIGH

MONITORING & TESTING

- [ ] Track and monitor all access to network resources and cardholder data
  HIGH
- [ ] Regularly test security systems and processes: run vulnerability scans quarterly
  HIGH
- [ ] Review logs daily for suspicious activity
  HIGH

POLICY & TRAINING

- [ ] Maintain an information security policy for all staff
  HIGH
- [ ] Train all employees who handle card data on PCI security practices
  HIGH

COMPLIANCE REPORTING

- [ ] Complete PCI Self-Assessment Questionnaire (SAQ) annually
  HIGH
- [ ] Run approved quarterly network vulnerability scans (ASV scans if required)
  HIGH

THIRD-PARTY VENDORS

- [ ] Verify your payment processor and gateway are PCI-compliant
  HIGH
- [ ] Review contracts with payment vendors for PCI responsibility clauses