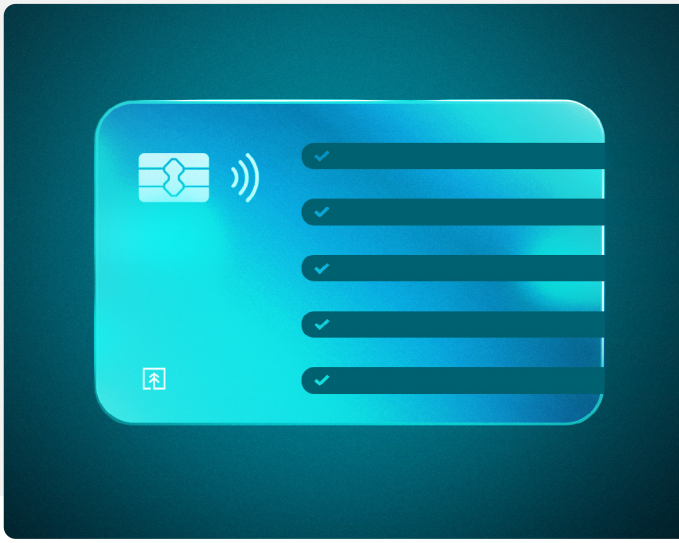
JSCAPE by Redwood | Redwood

PCI DSS
compliance checklist

Use this convenient checklist to ensure your organization fully complies with the Payment Card Industry Data Security Standard (PCI DSS) and avoids fines, legal action and reputational damage.



- [ ] **Be proactive about employee awareness and training.**

  Provide regular security training on PCI DSS requirements and best practices.
  Cover topics like phishing scams, password management and data handling procedures.

- [ ] **Engage in secure software development.**

  Follow secure coding practices and regularly test for vulnerabilities in applications that handle cardholder data: incorporate code reviews, penetration testing and vulnerability scanning throughout the lifecycle.

- [ ] **Securely configure your network.**

  Install firewalls and routers and change default system passwords and security settings to prevent unauthorized access. Regularly review and update network security configurations to maintain a strong security posture.

- [ ] **Prioritize third-party security and fully vet potential partners.**

  Make sure your third-party vendors also comply with PCI DSS if they handle cardholder data, as they're an extension of your own security perimeter. Include clear security requirements and provisions for audits in contracts. Ask for a trust package and what to expect if a security incident occurs.

- [ ] **Perform regular vulnerability management.**

  Keep software and systems up to date with patches to address known vulnerabilities.
  Use antivirus/anti-malware tools to create a robust defense against evolving cyberattacks.

Develop a comprehensive incident response plan.

Have a clear plan for responding to data breaches or security incidents, and test it regularly. Outline roles, responsibilities, communication protocols and steps for recovery and remediation.

Use proper data retention and disposal procedures.

Retain cardholder data only as necessary and securely dispose of it when no longer needed to minimize the risk of a breach. Implement secure data destruction methods, such as wiping or shredding.

Set up access control and user authentication.

Limit access to sensitive data based on business needs, following the principles of least privilege and role-based access control (RBAC). Require multi-factor authentication (MFA) for users accessing cardholder data.

Encrypt cardholder data.

Use strong encryption (e.g., AES-256) to store and transmit cardholder data. This renders it unreadable to unauthorized individuals and minimizes the impact of a potential breach.

Monitor and log activity.

Log and monitor all access to cardholder data for suspicious activity to enable timely detection and response to potential threats. Configure alerts for suspicious activity to ensure prompt notification and investigation.