SMART CHOICE COMMUNICATIONS

PCI COMPLIANCE

The Payment Card Industry Data Security Standard (PCI DSS) requires that any company handling cardholder information must securely host the data through a PCI compliant hosting provider. If your company accepts credit card or debit payments, you must ensure cardholder information stays protected from potential data breaches, leaks and hacks.

As a PCI Compliant hosting provider, Smart Choice safeguards your sensitive data through built-in encryption, proactive monitoring and advanced software. We securely store your data in our private SCC Cloud–powered by our fully-redundant data centers–and provide offsite backup with disaster recovery protocols in place.

BENEFITS

Compliance in the Cloud

SCC's private cloud stores your most sensitive data and ensures protection through built-in encryption and advanced security software.

Fully Redundant Data Centers

Our nationwide, fully-redundant data centers are 100% compliant with PCI DSS data security standards.

Disaster Recovery

We provide offsite backup and cloud-based disaster recovery options to ensure your data and applications are fully protected.

Proactive Updates and Safeguards

We provide updates and patches to stay up-to-date with the latest security protocols and ensure all necessary safeguards are in place at all times.

24/7/365 Support

Our 100% U.S. based support team is available 24/7/365 to answer any questions and provide support.

SMART CHOICE COMMUNICATIONS

PCI COMPLIANCE

Smart Choice is in compliance with all 12 of the PCI DSS requirements. They are as follows:

BUILD AND MAINTAIN A SECURE NETWORK

1: Install and maintain a firewall configuration to protect cardholder data
2: Do not use vendor-supplied defaults for system passwords and other security parameters

PROTECT CARDHOLDER DATA

3: Protect stored cardholder data
4: Encrypt transmission of cardholder data across open, public networks

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

5: Use and regularly update anti-virus software
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: Assign a unique ID to each person with computer access
9: Restrict physical access to cardholder data

REGULARLY MONITOR AND TEST NETWORKS

10: Track and monitor all access to network resources and cardholder data
11: Regularly test security systems and processes

MAINTAIN AN INFORMATION SECURITY POLICY

12: Maintain a policy that addresses information security