Steps to PCI Compliance

Any company that interacts with cardholder data must be within PCI compliance at all times. Here are the compliance essentials:

Use and Maintain Firewalls and Anti-Virus Protection
Install up-to-date, trusted firewall, anti-virus, and malware protection software to secure your systems and networks.

Proper Password Protections
Create system passwords that are unique, use special characters, upper and lowercase letters, numbers, and arranged so they cannot be guessed or easily memorized.

Protect Cardholder Data
Dispose of any retained cardholder data safely and regularly, or do not store this data at all.

Encrypt Transmitted Data
Transmitted data must be encrypted when sent over open networks to keep digital data confidential.

Properly Updated Software
Update and upgrade to new security releases or patches for security holes and protect against newest vulnerabilities.

Restrict Data and Physical Access
Limit sensitive data access with security codes and have security strategies that restrict physical access to data on servers, networks, and workstations.

Unique IDs for Access
Assign unique user IDs for employees and contractors. If a problem occurs it can be traced to the responsible party.

Create and Maintain Access Logs
Access logs help record security breach instances and have all the pertinent information about the vulnerability.

Scan and Test for Vulnerabilities
Penetration testing and vulnerability scanning are necessary to find flaws in servers, networks, and systems.

Document Policies
Complete yearly self-assessment of security policies for online and on-site security forms, procedures, and policies.