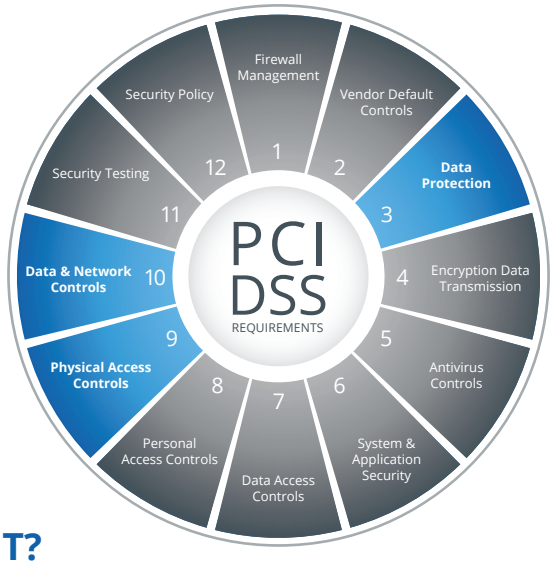
WipeDrive and PCI DSS Compliance

Digital payments are the norm in our society, with debit and credit cards providing easy access to our bank accounts and lines of credit. The speed, security, and efficiency of credit card payments continue to improve; however, as happens with all financial systems, customer credit card data theft is on the rise as well.



Since 2006, there have been standards in place that require companies to manage customer credit card information by a strict set of requirements and by providing certifications to those businesses which comply with the PCI DSS standards. The Payment Card Industry Data Security Standard outlines responsible data practices and requirements for PCI DSS Certification.

WHAT DOES IT MEAN TO BE PCI-DSS COMPLIANT?

Businesses that achieve PCI DSS certification enjoy access to secure credit card networks and the trust of customers paying digitally. In order to be in PCI DSS compliance, your company must:

- **Maintain a secure network** to protect customer's credit card and financial information. The network must have a firewall configured and tested that will keep cardholder information secure. If you host your transactions through a vendor, they must meet PCI requirements.
- **Encrypt customer financial data** during transmission across public networks. By transforming transaction data into ciphertext, which requires a cryptographic key to unlock, data encryption protects sensitive information as it travels through the web.
- **Protect stored cardholder data** behind unique passwords and security protocols. Systems must be protected against malware and viruses through current antivirus software. Network access to credit card data must be on a need-to-know basis, and physical access must be restricted.

- **Limit the storage of cardholder data** to necessary business reasons. Data disposal, destruction, and retention policies must be in place to meet these specific requirements:
  - Data may not be retained longer than required to meet industry regulations, business needs, or legal requirements.
  - Data must be deleted in a secure manner, documented in the data processes. Sensitive card authentication information may not be stored, even if encrypted.
  - Any sensitive authentication data that may be received must be destroyed in a way that makes it unrecoverable after transaction authentication is complete.
  - Data stored must be reviewed quarterly, at minimum, to ensure that any cardholder information that is past its retention date is securely destroyed.
  - Credit card companies themselves are allowed to store the authentication data when there is business justification and that data is kept secure.

PROFESSIONAL PARTNERS IN COMPLIANCE

Many organizations find it hard to meet PCI DSS compliance. At WhiteCanyon Software, we provide erasure software for businesses and government organizations as a PCI DSS certified partner.

With software security solutions that meet or exceed the PCI requirements, you can protect your business reputation, avoid fines, and retain your ability to accept credit and debit cards as payment. Contact us +44 (0) 345 340 3105 today for more information.

Sources:

1. https://www.whitecanyon.com/resources/white-papers/meeting-pcidss-requirements