WIPEDRIVE
ENTERPRISE

WipeDrive is Fundamental in Helping Organizations Meet PCI DSS Requirements

www.WhiteCanyon.com | Sales@WhiteCanyon.com | 1 (801) 224-8900

Overview

New data breach strategies and attacks have made it imperative that standards be put in place to protect credit card data. The Payment Card Industry Data Security Standard (PCI DSS) is an ongoing regulation started in 2006 to ensure that all companies that accept, process, store or transmit credit card information do so in a secure environment. The PCI DSS compliance standard applies to all industries, especially retailers, banks, financial service providers, restaurants, online stores, hotels and many more.

Certain components of PCI DSS are addressed by the WipeDrive erasure solution. This report explains those Requirements and WipeDrive's role in providing compliance.

PCI DSS REQUIREMENTS

Build and Maintain a Secure Network	1. Install & maintain a firewall configuration to protect card holder 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 acress open. public networks.
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update antivirus software or programs.
	6. Develop and maintain secure systems and applications.
Implement Strong Control Access Measures	7. Restrict access to cardholder data to business need to know.
	8. Identify & authenticate access to system components.
	9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	**10.** Track & monitor all access to network resources and cardholder data.
	11. Regularly test security systems and processes.
Maintain an Info Security Policy	12. Maintain a policy that addresses information security for all personnel.

Blue represent specific requirements that WipeDrive can help with compliance.

REQUIREMENT 3: PROTECT STORED CARDHOLDER DATA

PCI DSS V3.2 REQUIREMENT	HOW WIPEDRIVE SATISFIES THIS REQUIREMENT:
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	WipeDrive Enterprise provides an end of life and drive reallocation solution for IT assets used to store cardholder data. WipeDrive can erase cardholder data on laptops, workstations, servers and mobile devices. WipeDrive provides automatic data erasure processes set to meet the internal data security policy and requirement in an organization. **Specific Examples:** WipeDrive can be deployed throughout a datacenter to erase drives on a regular scheduled basis to ensure all cardholder data has been sanitized prior to decommissioning and shredding of the drives.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely	WipeDrive Enterprise implement internal and a patented 3rd party cryptographic erasure process and is a certified erasure tool for end of life IT asset disposition. **Specific Examples:** WipeDrive Enterprise can be deployed to laptops storing credit card data and permanently wipe the data from the devices. The process includes providing an audit report for archival reports. WipeDrive Enterprise can also be deployed when IT assets are reallocated to ensure all credit card data has been securely erased prior to the new assignment.

REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

PCI DSS V3.2 REQUIREMENT	HOW WIPEDRIVE SATISFIES THIS REQUIREMENT:
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	WipeDrive Enterprise is compliant with the National Institute of Standards and Technology (NIST) 800-88 erasure requirements of Clear and Purge for SSDs and Hard Drives. WipeDrive is also certified by Common Criteria EAL2+ as an international solution for data sanitization. The audit reports of each wipe are hash encrypted to ensure accurate reporting. **Specific Examples:** WipeDrive Enterprise can be deployed via PXE Network to all IT assets leaving a facility. The wiping process will ensure all credit card data has been securely wiped from each system. Each of the client computer's audit reports are sent to a central repository for administrator review.

REQUIREMENT 10: TRACK AND MONITOR NETWORK ACCESS

PCI DSS V3.2 REQUIREMENT	HOW WIPEDRIVE SATISFIES THIS REQUIREMENT:
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived or restorable from backup).	WhiteCanyon is able to push all your audit logs to multiple locations with in your organization like a SQL database, email, file share, FTP, etc. This way you have your audit reports with in your firewall. Every time a data erasure is performed, a report is created and stored for compliance, audit, reporting, verification, and retention purposes.

WhiteCanyon Software is the leading provider of secure data sanitization technology for storage media. As storage technology continues to advance, and the focus on data protection increases, WhiteCanyon will continue to provide a solution that exceeds industry standards.

There is a significant difference between software claiming to be "in compliance" with standards and software that is "certified" by recognized security organizations. Our enterprise class software is the most highly certified tool on the market. White Canyon has been through the rigorous process to gain these certification so you can rest easy, knowing your data has been securely deleted.

If you have any further questions about how WhiteCanyon can help you with your data erasure needs, please contact our Sales Team at (801) 224-2952.