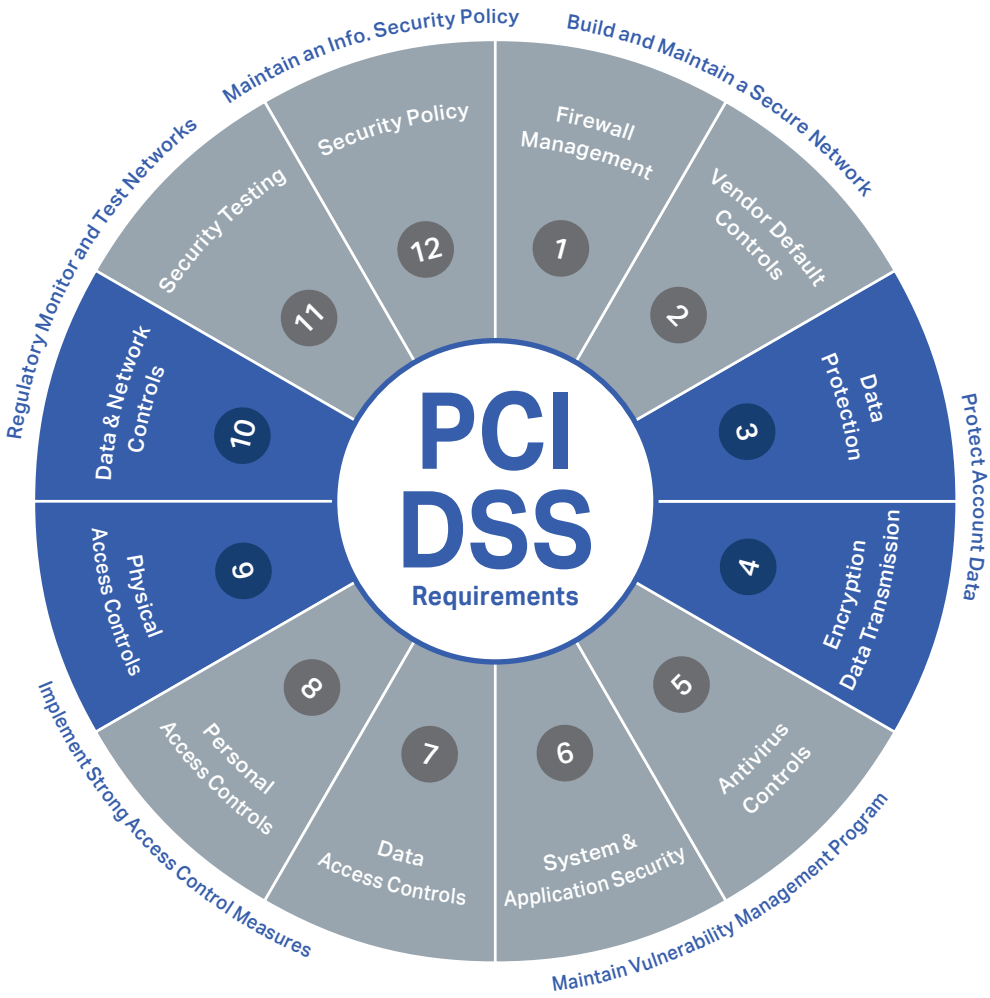
blancco

Meet PCI DSS v4.0.1 Cardholder Data Erasure Requirements with Blancco

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security guidelines designed to ensure that all companies processing, storing, or transmitting payment card information, safeguard cardholder data (CHD) against the risk of stored account data being compromised.

As with previous versions, the most recent update of the guidelines, PCI DSS v4.0.1., maintains that companies must satisfy data destruction and minimization requirements.

Need to meet the PCI DSS requirements for the disposal of cardholder data? Blancco can help. The following compliance checklist sets out some of the relevant requirements and the Blancco solutions that address them.



Blue segments represent specific requirements that Blancco can help satisfy.

blancco

Requirement 3: Protect Stored Account Data

PCI DSS V4.0.1 REQUIREMENT	BLANCCO SOLUTION	HOW BLANCCO HELPS
3.2.1 - "Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: ☑ Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy ☑ A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable" **Also stated within the requirements:** "The deletion function in most operating systems is not 'secure deletion' as it allows deleted data to be recovered, so instead, a dedicated secure deletion function or application must be used to make data unrecoverable."	☑ Blancco File Eraser ☑ Blancco Virtual Machine Eraser ☑ Blancco LUN Eraser ☑ Blancco Drive Eraser	Blancco solutions go beyond mere "deletion." Our tools securely and permanently erase data, making it unrecoverable from computers, drives, and live environments. Blancco solutions also enable programmatic processes by automating data erasure according to policy and requirement. **Example:** Blancco File Eraser supports this PCI requirement with scripting and scheduling. Merchants can erase private credit card data on a regular, ongoing basis to ensure and prove compliance with erasure reports. Scheduling the ongoing sanitization of assets enforces data retention policies in a scalable, automated way. Blancco File Eraser, Virtual Machine Eraser, and LUN Eraser all offer coverage in virtual machine, active storage, and hypervisor environments. Blancco Drive Eraser supports full wiping of cardholder data and sensitive authentication data (SAD) on HDDs and SSDs once those devices reach end-of-life.
3.3 - "SAD is not stored after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process." N.B., it is permissible for issuers and companies that support issuing services to store sensitive authentication data if: ☑ There is a business justification ☑ The data is stored securely	☑ Blancco File Eraser ☑ Blancco Virtual Machine Eraser ☑ Blancco LUN Eraser	Blancco erasure products support cryptographic erasure techniques (when they exist) and can also apply additional erasure processes to increase the security when data is no longer needed or cannot be kept. **Example:** Blancco File Eraser can be used to erase files carrying payment card data in a Windows or Unix environment, while Blancco Virtual Machine Eraser supports this process by erasing data on hypervisor layers within virtual machines without disruption to business operations. Blancco LUN Eraser allows organizations to erase data in active storage environments while allowing the operating system to remain intact

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

PCI DSS V4.0.1 REQUIREMENT	BLANCCO SOLUTION	HOW BLANCCO HELPS
4.2.2 - "There could be occurrences where an entity receives unsolicited cardholder data via an insecure communication channel that was not intended for transmissions of sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or delete the cardholder data and implement measures to prevent the channel from being used for cardholder data."	☑ Blancco File Eraser ☑ Blancco Virtual Machine Eraser ☑ Blancco LUN Eraser	If unsolicited data is received via insecure channels, merchants may choose to delete the data. As PCI DSS v4.0.1 explains elsewhere in the guidelines, however, the data deletion function in most operating systems is insecure, which means a dedicated secure erasure solution should be used.

Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS V4.0.1 REQUIREMENT	BLANCCO SOLUTION	HOW BLANCCO HELPS
9.4.7 - "Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: ☑ The electronic media is destroyed ☑ The cardholder data is rendered unrecoverable so that it cannot be reconstructed"	☑ Blancco Virtual Machine Eraser ☑ Blancco LUN Eraser ☑ Blancco Drive Eraser ☑ Blancco Eraser for Apple Devices	Blancco products meet the highest international media sanitization requirements, supporting merchants to securely erase electronic media in line with PCI DSS requirement 9.4.7. Blancco Drive Eraser in particular sanitizes drives in line with Clear and Purge level erasure as prescribed in the National Institute of Standards and Technology (NIST) 800-88, REV. 1 standard and the newer IEEE 2883-2022 standard. All data erasures are certified by 100% tamper-proof reports.

blancco

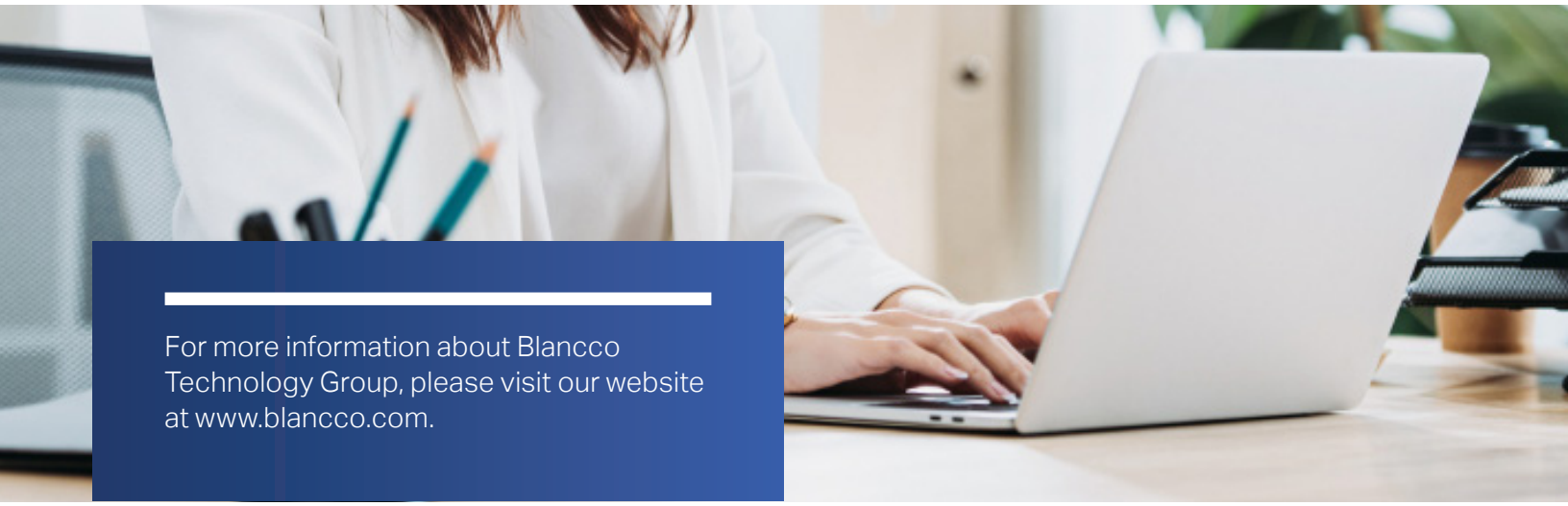
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

PCI DSS V4.0.1 REQUIREMENT	BLANCCO SOLUTION	HOW BLANCCO HELPS
"Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs on all system components and in the cardholder data environment (CDE) allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is difficult, if not impossible, without system activity logs. This requirement applies to user activities, including those by employees, contractors, consultants, and internal and external vendors, and other third parties (for example, those providing support or maintenance services)."	☑ Blancco Management Portal	Blancco Management Portal is a centralized platform that allows you to manage data erasure across all IT assets, with a single program for consolidated reporting. Every time a data erasure is performed, a report is created and stored for compliance, audit, reporting, verification, and retention purposes.

For over 20 years, Blancco has offered solutions that support compliance with data protection and privacy regulations like PCI DSS v4.0.1.

We support organizations in all industries to stay compliant with relevant regulations with data erasure solutions that satisfy (and often exceed) those requirements.

Contact us today for additional information about how we can help you pass your next data security audit.



For more information about Blancco Technology Group, please visit our website at www.blancco.com.