

Does hashing of passwords meet the intent of PCI DSS Requirement 8.3.2?

PCI SSC FAQ | Article 1253 | July 2025

Yes. Using strong cryptography to hash the password meets the intent of the PCI DSS Requirement 8.3.2, which requires that all authentication factors be rendered unreadable during transmission and storage using strong cryptography.

This requirement is designed to prevent unauthorized access to these authentication factors, both in storage and as they traverse the network. When implemented properly, hashing ensures that passwords cannot be easily recovered or misused, even if the data is compromised.

Please refer to the PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information on hashing.

Source: <https://www.pcisecuritystandards.org/faqs/1253/>