

Should cardholder data be encrypted while in memory?

PCI SSC FAQ | Article 1042 | December 2022

If the cardholder data is stored in non-persistent memory (e.g. RAM), encryption of cardholder data is not required. However, proper controls must be in place to ensure that memory maintains a non-persistent state. For example, if the data in memory is being written to a file, then appropriate PCI DSS requirements are applicable to that file.

Data should be removed from volatile memory once the business purpose (for example, the associated transaction) is complete. In the case that data storage becomes persistent, all applicable PCI DSS requirements will apply, including encryption of stored data.

PCI SSC recommends engaging a Qualified Security Assessor (QSA) for guidance as to whether a specific implementation will satisfy this requirement. For a list of QSAs, please visit: https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

Source: <https://www.pcisecuritystandards.org/faqs/1042/>