PCI DSS Guidelines for Temporary Data Storage

This document outlines PCI DSS-compliant practices for storing sensitive data (such as messages containing cardholder data) temporarily during transaction processing.

Key PCI DSS Requirements:

1. Sensitive Authentication Data (SAD):
   - Must never be stored after authorization, even if encrypted (e.g., CVV/CVC).
   - Temporary storage prior to authorization must be securely deleted immediately after authorization.

2. Cardholder Data (CHD) including PAN:
   - Can be stored temporarily if business-justified and encrypted using strong cryptography (e.g., AES-256).
   - Must be removed as soon as it's no longer needed.

3. Storage Duration:
   - PCI DSS does not define an exact time limit.
   - Temporary data should be retained only for the shortest time possible (typically seconds or a few minutes).
   - Example: Set automated cleanup jobs to remove or nullify data after 15 minutes.

4. Logging:
   - Do not log full PAN, CVV, or content.
   - Log only metadata such as message ID, status, and timestamp.

5. Best Practices:
   - Apply multi-layer encryption.
   - Use role-based access control.
   - Schedule DB cleanup jobs for old/stale entries.
   - Document data retention and removal policies.

Compliance Summary:

- Temporary storage: Allowed with justification and encryption.
- CVV/CVC: Never allowed to be stored post-authorization.
- Cleanup: Required immediately after data is processed.
- Logging: Only metadata should be logged.

This document can be used for internal security teams and PCI auditors to validate data handling strategy.