1. Introduction

This document outlines the cryptographic key management procedures for [Company Name], a payment gateway company. These procedures ensure the secure generation, storage, use, rotation, and destruction of cryptographic keys used to protect sensitive payment data. This document adheres to industry best practices and relevant security standards.

2. Key Roles and Responsibilities

Security Officer: Oversees the overall key management program and ensures compliance with this document.

Key Custodian: Manages the secure storage and access controls for cryptographic keys.

System Administrators: Generate and manage keys for specific systems and applications.

Security Team: Conducts regular audits and reviews of key management procedures.

3. Key Lifecycle Management

3.1 Key Generation

Keys are generated using a Hardware Security Module (HSM) or a cryptographically secure random number generator.

Key generation parameters are chosen based on the intended use of the key and current cryptographic standards.

The generation process is documented and auditable.

3.2 Key Storage

Keys are stored in a secure HSM or a Key Management System (KMS) that provides tamper-evident and access-controlled storage.

Keys are never stored in plain text. They are encrypted using strong algorithms and appropriate key lengths.

Access to keys is restricted based on the principle of least privilege.

3.3 Key Usage

Keys are used only for their intended purpose and within approved applications.

The use of keys is logged and monitored for suspicious activity.

Keys are never shared with unauthorized parties.

3.4 Key Rotation

Keys are rotated periodically based on industry best practices and risk assessments.

The rotation process is documented and ensures the secure destruction of old keys before new keys are activated.

3.5 Key Destruction

Keys are securely destroyed at the end of their lifecycle or upon compromise.

Destruction methods are documented and ensure that keys are unrecoverable.

4. Key Compromise Procedures

A documented incident response plan outlines the steps to be taken in case of a suspected key compromise.

The plan includes actions for containment, eradication, and recovery.

The Security Officer is notified immediately in case of a suspected compromise.

Compromised keys are immediately revoked and replaced with new keys.

5. Audits and Reviews

Regular audits are conducted to ensure compliance with this key management procedure document.

Audits assess the effectiveness of key management controls and identify any potential vulnerabilities.

The key management program is reviewed periodically to reflect changes in technology or security threats.

6. Training and Awareness

Personnel involved in key management activities are trained on these procedures.

Training covers key security principles, key handling practices, and incident response procedures.

Regular awareness programs educate employees on the importance of key security.

7. References

National Institute of Standards and Technology (NIST) Special Publication 800-57 National Institute of Standards and Technology (NIST): https://csrc.nist.gov/pubs/sp/800/57/pt1/r5/final)

Payment Card Industry Data Security Standard (PCI DSS) PCI Security Standards Council: https://www.pcisecuritystandards.org/

8. Revision History

This document will be reviewed and updated periodically to reflect changes in the company's environment, security threats, or industry standards.

The revision history will be maintained to track changes made to the document.

9. Appendix

The appendix may contain additional information such as:

Specific key generation parameters for different key types

Access control matrix for key management roles

Key destruction procedures