

Cryptographic Key Management Policy

Reference: PCI POL 3.2

DocumentKits Issue No: 1.1

Organisation Issue No:

DocumentKits Issue Date: 29/06/2020

Organisation Issue Date:

1. Scope

All cryptographic keys used by Organisation Name.

"The controls that you adopt will depend very much on your risk assessment and on the precise circumstances in which you are deploying them, as well as on the type of controls that you are using. The range of options is too great for the creation of a template; you need to decide what you are going to do and document it here."

2. Responsibilities

2.1 The Information Security Manager is responsible for maintaining the schedule of required keys in line with the risk assessment, this procedure and evolving security environment.

2.2

"Individual asset owners"

are responsible for ensuring that the required cryptographic control is applied.

2.3 Key custodians consist of

"Enter the roles who are custodians. A minimum of two should be selected."

3. Definitions

3.1 Strong encryption keys are where the key length is such, that the resulting work factor is high enough to protect information for the period defined in the data retention and disposal policy.

3.2 The algorithms and key lengths that form strong cryptography are constantly changing as new vulnerabilities and weaknesses are discovered, and as new methods of breaking encryption are developed; as well as the speed and power of computational devices used to perform this increases with time.

3.3 The deployed cryptography should meet current recommendations from the PCI SSC and bodies such as GCHQ, NIST and other standard and trade bodies.

4. Requirements

4.1 Strong encryption keys are generated by

"Document the procedure you use. A fully automated process may be in use. "

4.2 Cryptographic keys are distributed securely via

"Document the procedure you use."

4.3 Access to keys is restricted by the Head of IT (CIO) to the fewest number of custodians considered necessary to both ensure security and enable Organisation Name to function effectively.

4.4 Cryptographic keys are stored securely

"Enter where the cryptographic keys are stored"

and in as few locations as the Head of IT (CIO) considers possible. Keys are stored in encrypted format and key-encrypting keys are stored separately from data-encrypting keys.

4.5 Cryptographic keys are changed periodically

"Specify the life expectations of your keys and which guidelines those are based on, such as the NIST Key Management Guidelines. Also detail how they are changed, e.g. automatically."

4.6 Keys which have been compromised or believed to have been compromised are replaced immediately by

"Specify who"

The Head of IT (CIO) is responsible for the retirement of old keys, archived keys are secured/stored

"Where?"

and destroyed securely when no longer required.

4.7

"Name roles of those involved in manual key generation, if used, must be at least 2 individuals"

are responsible for the creation of keys ensuring split knowledge and dual control of keys.

4.8 Unauthorised substitution keys are prevented via physical and logical access to the key generating procedures and mechanisms.

"Describe technically how this is done."

4.9 Encryption keys are managed by

"Document the process"

4.10 Key custodians must sign the [Cryptographic Key Custodian Acceptance Form](#) specifying that they understand and accept their key custodian responsibilities.

4.11 Organisation Name maintains a documented description of cryptographic architecture

"Reference document name here"

that includes: inventories of and HSM's or other devices used for key management, details of cryptographic key usage, and details of algorithms, protocols, key strengths, and key expiry dates.

Document Owner and Approval

The Information Security Manager is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) – electronic and physical – where this document is available"

Its approval status can be viewed in the [Master List of Document Approval](#).