

## Stored Cardholder Data Policy

<b>Approved By</b> <hr/> \\S\ James Palmer CSC Loss Prevention Director <hr/> December 31, 2014 Date	<b>PCI Policy # 1900    Version # 1.0</b>  <b>Effective Date:</b> 12/31/2014
--	--

### 1.0 Purpose:

The purpose is to implement policies and procedures to ensure that all stored cardholder data is adequately protected.

### 2.0 Compliance:

PCI DSS Requirement 3

### 3.0 Scope:

This policy applies to MWR Program in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit sensitive information.

### 4.0 Policy:

Procedures for the logical and physical protection of cardholder data will be documented, implemented and known to all affected parties.

### Cardholder Data Storage Rules

All cardholder data storage will be kept to a minimum as limited by business, legal, and regulatory requirements. Storage amount and retention time will be documented in the Corporate Data Retention Policy.

Sensitive authentication data (SAD) must not be stored after authorization even if there is no PAN in the environment. SAD that is received is to be rendered unrecoverable upon completion of authorization process.

A quarterly automatic or manual process for identifying and securely deleting cardholder data that exceeds defined retention requirements will be documented and performed.

Full contents of any track data and the personal identification number (PIN) cannot be stored.

The PAN (primary cardholder account number) will be masked when displayed (the first six and last four digits are the maximum number of digits that will be displayed). The only exception will be those employees with a business need to see the entire PAN.

PAN will be rendered unreadable anywhere it is stored by using one of the following:

- Strong one-way hash functions (hashed index)
- Truncation
- Index tokens and pads
- Strong cryptography with key management processes.

Encryption keys used for encryption of cardholder data will be protected by restricting access to the keys and storing the keys securely in one or more of the following forms:

- Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key
- Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of interaction device)
- As at least two full-length key components or key shares, in accordance with an industry-accepted method.

Logical access for disk encryption must be managed separately and independently of the native operating system authentication and access control mechanisms. Decryption keys must not be associated with user accounts.

Key management processes and procedures for keys used in encryption will be fully documented and implemented. These process and procedures will include the generation of strong keys, secure key distribution and storage, periodic change of keys, destruction of old keys, dual control and split knowledge of keys, replacement of suspected compromised keys, and the signing of a form by key custodians stating that they understand and accept their key-custodian responsibilities.

### **5.0 Responsibility:**

The MWR Director/Officer is responsible for leading compliance activities that bring the Coast Guard – MWR into compliance with the PCI Data Security Standards and other applicable regulations.

### **6.0 Form(s):**

Form 1901 – Key Custodian Acceptance Form  
Form 1902 – Hardware System Components Form  
Corporate Data Retention Policy (*you will need to create*)  
Key Management Procedures (*you will need to create*)

### **7.0 Definition(s):**

Definitions for technical terms can be found in Appendix A of your MWR PCI Compliance Workbook.

### **8.0 Policy History:**

Initial effective date: 12/31/2014