CREDIT CARD SECURITY POLICIES
PCI DSS 3.1 – DATA RETENTION AND DISPOSAL POLICY

Version 1.0 – June 30, 2015

CONFIDENTIAL INFORMATION
This document is the property of Missouri Botanical Garden; it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of Missouri Botanical Garden.
### Revision History

<table>
<thead>
<tr>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td>June 30, 2015</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS

1. INTRODUCTION ...................................................................................................... 4
   1.1 Scope ......................................................................................................................... 4
   1.2 Description of Data and Scope for Cardholder Environment ............................................. 4
   1.3 Description of Key Terms and Phrases ............................................................................. 4
   1.4 Types of Data .............................................................................................................. 6

2. PROCEDURE .............................................................................................................. 6
   2.1 Procedure for Obtaining Data ......................................................................................... 7
   2.2 Procedure for Protecting Data ........................................................................................ 7
   2.3 Procedure for Accessing, Modifying or Transferring Cardholder Data .............................. 7
   2.4 Provisions and Procedures for Retaining Data ................................................................. 8
   2.5 Provisions and Procedures for Disposing of and Destroying Data ..................................... 8
   2.6 Responsible Parties for Data Retention Activities ......................................................... 8
   2.7 Responsible Parties for Data Disposal Activities ........................................................... 9
   2.8 Responsibility for Policy Maintenance ............................................................................. 9

3. DISPLAYING PRIMARY ACCOUNT NUMBER (PAN) ......................................... 9
   3.1 Policy ......................................................................................................................... 9
   3.2 Procedure .................................................................................................................... 10
   3.3 Responsibility for Policy Maintenance .......................................................................... 10

4. PRIMARY ACCOUNT NUMBER (PAN) SYSTEM PROTECTION .................... 10
   4.1 Policy ......................................................................................................................... 10
   4.2 Procedure .................................................................................................................... 10
   4.3 System used for Protecting the PAN .............................................................................. 11
   4.4 Encryption .................................................................................................................. 11
   4.5 Other Means Utilized for Protecting the PAN ................................................................. 11
   4.6 Responsibility for Policy Maintenance .......................................................................... 11

5. PROTECTION OF KEYS USED FOR ENCRYPTION OF CARDHOLDER DATA .......................................................... 11
   5.1 Policy ......................................................................................................................... 11
   5.2 Access to Cryptographic Keys ...................................................................................... 11
   5.3 Storage and Location of Cryptographic Keys ................................................................. 12
   5.4 Responsibility for Policy Maintenance ........................................................................... 12

6. KEY MANAGEMENT POLICY AND PROCEDURES ........................................ 12
   6.1 Policy ......................................................................................................................... 12
   6.2 Procedure .................................................................................................................... 13
   6.3 General Description of System Components that Incorporate Key-Management .......... 13
   6.4 Responsibility for Policy Maintenance ........................................................................... 16
1. INTRODUCTION

1.1 Scope

The Data Retention and Disposal policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 2.0):

- Limiting data storage amount and retention time to that which is required for legal, regulatory and business requirements
- Processes are in place for secure disposal of data when no longer needed for legal, regulatory and business requirements.
- Retention requirements are in place and documented accordingly for all legal, regulatory and business requirements
- An automatically or manually executed quarterly process is in place for identifying and securely removing cardholder data that exceeds the defined legal, regulatory and business requirements.

1.2 Description of Data and Scope for Cardholder Environment

Cardholder data, as defined by the Payment Card Industry Security Standards Council (PCI SSC) Glossary of Terms, includes, at a minimum the Primary Account Number (PAN), and may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or the service code. Additionally, cardholder data may also include Sensitive Authentication Data, such as security-related information (card validation codes/values, full magnetic stripe data, PINs and PIN blocks) used to authenticate cardholders, which appears in plain-text or otherwise unprotected form. This cardholder data may reside in numerous places throughout the cardholder environment.

1.3 Description of Key Terms and Phrases

(Security Standards Council Glossary of Terms, 2008)

- **Access Control:** Mechanisms that limit availability of information or information-processing resources only to authorized persons or applications
- **Cardholder Data:** The Primary Account Number (PAN) may also appear in the form of the full PAN, plus any of the following:
  - Cardholder name
  - Expiration date
  - Service code
- **Card Verification Code or Value:** Data element on a card's magnetic stripe that uses a secure cryptographic process to protect data integrity on the stripe and reveals any alteration or counterfeiting (referred to as CAV, CVC, CVV or CSC, depending on payment card)
- **CAV** – Card Authentication Value (JCB payment cards)
- **CVC** – Card Validation Code (MasterCard payment cards)
• CVV – Card Verification Value (Visa and Discover payment cards)
• CSC – Card Security Code (American Express)
• Data: Pieces of information from which intelligible information is derived. Data are a collection of information or facts usually gathered as the result of experience, observation, experiment or processes within a computer system or premises. Data may consist of numbers, words or images, particularly as measurements or observations of a set of variables. They are often viewed as the lowest level of abstraction from which information and knowledge are derived.
• Database: Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets.
• Degaussing: Also called disk degaussing, it is the process or technique that demagnetizes the disk so that all data stored on the disk are permanently destroyed. • Disk Encryption: Technique or technology (either software or hardware) for encrypting all stored data on a device (e.g., hard disk, flash drive). Alternatively, File-Level Encryption or Column-Level Database Encryption is used to encrypt contents of specific files or columns.
• Encryption: Process of converting information into a form only intelligible to holders of a specific cryptographic key. The use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.
• Full Magnetic Stripe Data: Also referred to as track data. Data encoded in the magnetic stripe or chip is used for authorization during payment transactions. It can be the magnetic stripe image on a chip or the data on the Track 1 and/or Track 2 portion of the magnetic stripe. Entities must not retain full magnetic stripe data after obtaining transaction authorization.
• Primary Account Number (PAN): Acronym for primary account number and also referred to as account number. Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
• Removable Electronic Media: Media that store digitized data and can be easily removed and/or transported from one computer system to another. Examples of removable electronic media include CD-ROM, DVD-ROM, USB flash drives and removable hard drives.
• Sanitization: Process for deleting sensitive data from a file, device or system or for rendering data useless if accessed in an attack
• Secure Wipe: Also called secure delete, this is a program utility used to delete specific files permanently from a computer system.
• Sensitive Authentication Data: Security-related information (card validation codes/values, full magnetic stripe data, PINs and PIN blocks) used to authenticate cardholders, appearing in plain-text or otherwise unprotected form
• Service Code: Three- or four-digit value in magnetic stripe that follows the expiration date of the payment card on the track data. It is used for various such as defining service attributes, differentiating between international and national interchange or identifying usage restrictions.
• **System Components:** Any network component, server or application included in or connected to the cardholder data environment

1.4 Types of Data

Data may be in electronic media or in hardcopy format. The following is a list of where data and, specifically, cardholder data may reside:

1.4.1. Electronic Media

Electronic media are the bits and bytes contained in hard drives, Random Access Memory (RAM), Read-Only Memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment and various other media.

- Hard drives
- Tapes/media
- CDs
- DVDs
- Compact flash drives, SD
- Dynamic Random Access Memory (DRAM)
- Read-Only Memory (ROM and the different variations thereof)
- Random Access Memory (RAM)
- Flash cards
- USB drives, removable media, memory sticks

**Note:** Missouri Botanical Garden prohibits recording or storing cardholder data on CDs, DVDs, compact flash drives, SD cards, flash cards or USB drives. Removable hard drives and tapes are only used for backup purposes.

1.4.2. Hardcopy Format

Hardcopy media are physical representations of information. Paper printouts, printers, facsimile ribbons, drums and platens are all examples of hardcopy media.

- Paper receipts or other supporting hardcopy documents and receipts
- Credit card printouts from processing machines
- Invoices
- Purchase orders
- Offline hardcopy batch printouts
- Other hardcopy formats as identified by organizations

**Note:** The policies and procedures for handling and destruction of paper media containing cardholder data are documented in the *Media Storage and Destruction Policy* for each area that handles paper media.

2. Procedure

Missouri Botanical Garden developed and implemented a comprehensive program regarding data retention and disposal, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by Missouri Botanical Garden to ensure the Data Retention and Disposal policy initiatives are executed in a formal
manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources deemed critical by the organization.

2.1 Procedure for Obtaining Data

Data within the scope of the cardholder environment must be obtained in a secure manner so as not to compromise the information traversing public networks and internal Company-wide networks. Appropriate security-hardening and configuration standards are to be utilized throughout the entire network, which include but are not limited to the following system components: any network component (routers, switches, firewalls, load balancers, etc.), server or application(s) included in or connected to the Cardholder Data Environment.

Due diligence is exercised to ensure that other organizations associated with Missouri Botanical Garden’s Cardholder Data Environment also have appropriate security measures, standards and safeguards in place. This includes but is not limited to the following:

- Data centers and managed service providers
- Payment processors
- Payment gateways
- Client websites with ecommerce platforms

2.2 Procedure for Protecting Data

The transmission and subsequent storage of cardholder data is protected at all times. Protecting data includes any of the following:

- Use of HTTPS for secure cardholder transmission, beginning at point-of-sale activity from consumer
- Use of encryption for storage (disk, file, column encryption)
- For hardcopy format of cardholder data, adequate physical security controls (e.g., locked doors, limited access to file rooms, etc.) have been established by the Media Storage and Destruction Policy.

2.3 Procedure for Accessing, Modifying or Transferring Cardholder Data

Only authorized personnel may access, modify or transfer cardholder data. These activities are considered highly sensitive in nature, so they must be justifiable by a compelling business or operational requirement(s). Personnel authorized to conduct these activities include the following:

<table>
<thead>
<tr>
<th>PERSONNEL AUTHORIZED TO ACCESS, MODIFY OR TRANSFER CARDHOLDER DATA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name and Title</strong></td>
</tr>
<tr>
<td>Cassandra Nelson</td>
</tr>
<tr>
<td>Sr. Manager, System Administration</td>
</tr>
<tr>
<td>Michael Winstead</td>
</tr>
<tr>
<td>System Administrator</td>
</tr>
</tbody>
</table>
2.4 Provisions and Procedures for Retaining Data

Cardholder data will be retained in accordance with Payment Card Industry Data Security Standards (PCI DSS) provisions. Cardholder data will be retained as long as required for legal, regulatory or business requirement. After the business requirement for retention has been met and if no legal or regulatory requirement supercedes, the cardholder data shall be deleted within 30 days.

2.4.1 Cardholder Data Retention Review

Cardholder data retention will be reviewed quarterly to identify and secure delete stored cardholder data that exceeds the defined retention period.

2.5 Provisions and Procedures for Disposing of and Destroying Data

Once the maximum retention period has been reached for cardholder data, that data must be removed from all electronic media, and any hardcopy edition must be disposed of accordingly. Methods for disposal include the following:

- Purging and deleting cardholder data from all system components. This can be done by utilizing a secure wipe program in accordance with industry-accepted standards for secure deletion (i.e., degaussing). *System components* are defined as any network component, server or application included in or connected to the cardholder data environment.
- Destroying (cross-shredding) any cardholder data that is in a hardcopy format as prescribed in the Media Handling and Destruction Policy.
- For electronic media stored on system components that are no longer in use, these system components must have cardholder data disposed of through any one of the following procedures:
  - Utilizing a secure wipe program in accordance with industry-accepted standards for secure deletion Disintegration
  - Shredding (disk grinding device)
  - Incineration by a licensed incinerator
  - Pulverization

2.6 Backup Media Data Destruction

Once any media used for cardholder data backup is declared no longer useable, the data on the media will be completely wiped by utilizing a secure wipe program in accordance with industry-accepted standards for secure deletion.

2.7 Decommissioned Servers

Upon decommissioning of a physical server that stores cardholder data, the disk drives for that server will be completely wiped by utilizing a secure wipe program in accordance with industry-accepted standards for secure deletion.
2.8 Responsible Parties for Data Retention Activities

Only authorized personnel may establish and modify data retention periods. These activities are considered highly sensitive in nature, so they must be justifiable by a compelling business or operational requirement(s). Personnel authorized to conduct these activities include the following:

<table>
<thead>
<tr>
<th>Name and Title</th>
<th>Specific Responsibilities Relating to Data Retention of Cardholder Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chuck Miller, VP-IT and CIO</td>
<td>Establishes and modifies data retention period policy</td>
</tr>
</tbody>
</table>

2.9 Responsible Parties for Data Disposal Activities

Only authorized personnel (internal personnel and qualified external data destruction vendors) may dispose of cardholder data. These activities are considered highly sensitive in nature, so they must be justifiable by a compelling business or operational requirement(s). Personnel authorized to conduct these activities include the following:

<table>
<thead>
<tr>
<th>Name and Title</th>
<th>Specific Responsibilities Relating to Data Disposal of Cardholder Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cassandra Nelson, Sr. Manager, System Admin</td>
<td>System administration</td>
</tr>
<tr>
<td>Michael Westmoreland, System Admin</td>
<td>System administration</td>
</tr>
<tr>
<td>Bill Behns, Systems &amp; Telecommunications Admin</td>
<td>System administration; performs data backups</td>
</tr>
</tbody>
</table>

2.10 Responsibility for Policy Maintenance

The Vice President of IT is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

3. Displaying Primary Account Number (PAN)

3.1 Policy

The displaying of the Primary Account Number (PAN) adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security

- Primary Account Numbers (PAN) displayed onscreen will always be masked, with the first six and last four digits being the maximum number of digits to be displayed.
- If the Primary Account Numbers (PAN) must be fully displayed (all digits), they will only be permitted if necessitated by a compelling business requirement or legitimate business need.
3.2 Procedure

The displaying of the Primary Account Number (PAN) adheres to Payment Card Industry Data Security Standards (PCI DSS) requirements.

<table>
<thead>
<tr>
<th>System Components where PAN could be Displayed</th>
<th>Purpose for Having to Display PAN</th>
<th>Are Only the First Six Digits and Last Four Digits Displayed?</th>
<th>If Not, State the Business Reason or Need Why the Full PAN is Displayed</th>
</tr>
</thead>
<tbody>
<tr>
<td>EBMS/iEBMS</td>
<td>Needed for billing</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Raisers Edge</td>
<td>Needed for billing</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Galaxy</td>
<td>Needed for billing</td>
<td>Yes</td>
<td>N/A</td>
</tr>
<tr>
<td>Liberty</td>
<td>Needed for billing</td>
<td>Yes</td>
<td>N/A</td>
</tr>
</tbody>
</table>

3.3 Responsibility for Policy Maintenance

The Vice President of Information Technology is responsible for ensuring that the aforementioned policy is kept current as necessary for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

4. Primary Account Number (PAN) System Protection

4.1 Policy

The Primary Account Number (PAN) and the system used to protect it adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.1):

- The system used to protect the PAN is in place and meets all technical, operational and security requirements for the organization.
- Appropriate encryption (i.e., disk, file, column) is in place and is being used at all times for protection of the PAN, ultimately rendering the PAN unreadable while being stored, including on portable digital media, backup media and in logs.
- If encryption is not used, then Missouri Botanical Garden will ensure that the PAN is protected by other acceptable means such as hashing, truncating or indexing of tokens and pads.

4.2 Procedure

The Missouri Botanical Garden developed and implemented a comprehensive program regarding the Primary Account Number (PAN) system protection, which encompasses the categories and supporting activities listed below. These policy directives are fully enforced by the Garden for ensuring configuration standards initiatives are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources deemed critical by the Garden.
4.3 System used for Protecting the PAN
Raiser's Edge tokenizes the PAN after card authorization and only tokens are retained on the server.
The Galaxy, EBMS, and Liberty systems encrypt the PAN using AES 256 bit encryption.

4.4 Encryption
AES 256 bit encryption is used for storing PAN data.

4.5 Other Means Utilized for Protecting the PAN
Galaxy and Liberty display only the last 4 digits of the PAN.

4.6 Responsibility for Policy Maintenance
The Vice President of Information Technology is responsible for ensuring that the aforementioned policy is kept current as necessary for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

5. Protection of Keys used for Encryption of Cardholder Data

5.1 Policy
The protection of keys used for encryption of cardholder data adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.1):

- Access to cryptographic keys is restricted to the fewest number of custodians necessary.
- Cryptographic keys are stored in encrypted format and the key-encrypting keys are stored separately from data-encrypting keys.
- Keys are stored in the fewest possible locations and forms.

Procedure
The Missouri Botanical Garden developed and implemented a comprehensive program for the protection of keys used for encryption of cardholder data, which encompasses the categories and supporting activities listed below. These policy directives will be fully enforced by the Garden for ensuring protection of keys used for encryption of cardholder data initiatives are executed in a formal manner and on a consistent basis for all system components within the cardholder data environment and all other IT resources deemed critical by the Garden.

5.2 Access to Cryptographic Keys
Galaxy, EMBS and Liberty use AES 256 bit encryption. IT does not have access to the keys.

<table>
<thead>
<tr>
<th>PERSONNEL WITH ACCESS TO CRYPTOGRAPHIC KEYS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name and Title</td>
</tr>
</tbody>
</table>

11
5.3 Storage and Location of Cryptographic Keys

Secured Key database, stored on the IT Dept H: drive.

5.4 Responsibility for Policy Maintenance

The Vice President of Information Technology is responsible for ensuring that the aforementioned policy is kept current as necessary for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.

6. Key Management Policy and Procedures

6.1 Policy

The Missouri Botanical Garden developed key-management procedures for keys used for encryption of cardholder data utilizing industry-accepted standards for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives. The list of industry-leading security standards, benchmarks and frameworks to utilize includes but is not limited to the following:

- NIST Special Publication 800-57: Recommendation for Key Management Part 1
  http://csrc.nist.gov/publications
- NIST Special Publication 800-57: Recommendation for Key Management Part II – Best Practices for Key Management Organization

Additionally, key management procedures used for encryption of cardholder data must address the following requirements in order to ensure further compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (PCI DSS Requirements and Security Assessment Procedures, Version 3.1):

- Key-management procedures are implemented to require the generation of strong keys.
- Key-management procedures are implemented to require secure key distribution.
- Key-management procedures are implemented to require secure key storage.
- Key-management procedures are implemented to require periodic key changes at the end of the defined cryptoperiod, such as after a defined period of time has passed and/or after a certain amount of ciphertext has been produced by a given key.
Key-management procedures are implemented to require the retirement of old keys when the integrity of the keys has been weakened, thus implementing procedures such as archiving, destruction and revocation (as applicable) of keys.

Key-management procedures are implemented to require the replacement of known or suspected compromised keys. This action may be warranted with the departure of an employee who had access or knowledge of a clear-text key.

Key-management procedures are implemented to ensure that, if retired or replaced cryptographic keys are retained, they are not used for encryption operations.

Key-management procedures are implemented to require split knowledge and dual control of keys for any manual clear-text key-management procedures, such as requiring two or three people, each knowing only their own part of the key, to reconstruct the whole key.

Key-management procedures are implemented to require the prevention of unauthorized substitution of keys.

Key-management procedures are implemented to require key custodians to acknowledge (in writing or electronically) their understanding and acceptance of key custodial responsibilities.

6.2 Procedure

Discussed below is a series of established key-management procedures that are utilized throughout the cardholder environment for the Missouri Botanical Garden. Additional supporting documentation is also provided regarding the cardholder environment and all system components concerning key-management procedures.

6.3 General Description of System Components that Incorporate Key-Management

6.3.1. Generation and Secure Key Distribution

Generation and distribution of keys for the keys used for the encryption and decryption of data or other keys shall be as follows:

Keys shall be either

- Generated and subsequently distributed manually, using a public key transport mechanism or a previously distributed or agreed upon key-encrypting key
- Established using a key agreement scheme
- Determined by a key update process
- Derived from a master key

Keys determined by key generation methods shall be generated by an approved random number generation method, created from the previous key during a key update procedure or derived from a master key using an approved key derivation function.

When split knowledge procedures are used, the key shall exist as multiple key components. The keying material may be created and then split into components or may be created as separate components. Each key component shall provide no knowledge of the key value.
(i.e., each key component must appear to be randomly generated). If knowledge of \( k \) (where \( k \leq n \)) components is required to construct the original key, then knowledge of any \( k-1 \) key components shall provide no information about the original key other than, possibly, its length.

6.3.2. Secure Key Storage

From a scope perspective, secure key storage encompasses operational storage, backup storage and archival storage. Each of the three components plays a vital role in secure key storage for Payment Card Industry Data Security Standards (PCI DSS) compliance.

Missouri Botanical Garden’s operational secure key storage elements consist of the following:

For system components that require immediate access and availability to the keys for specific applications within the boundaries of system components as defined by the Payment Card Industry Data Security Standards (PCI DSS). These keys, which may be stored locally, must have strong physical security controls and logical security controls. Such controls preclude the writing of key values in the startup instructions or in the policy and procedures manual.

- Additionally, the use of root or a single authentication and authorization right that could be utilized by multiple users should also be prohibited.
- For users that do have access to keys within the operational storage environment, the system components must have acceptable audit and logging trails enabled and various dual controls as needed.
- If the keys are stored in a database repository, the Database Administrator (DBA) or any other individual with system administrative, super-user or privileged rights to the database should not have access to the respective keys in a clear text format.

The Missouri Botanical Garden’s backup storage secure key storage elements consist of the following:

- Keys are backed up to a secure and physical source of media, which is independent from the keys used in the operational storage environment.
- This allows for the retrieval of keys in the event of the operational storage environment being compromised.

The Missouri Botanical Garden’s archive storage secure key storage elements consist of the following:

- An archive for keying material shall provide both integrity and access control.
- Integrity is required in order to protect the archived material from unauthorized modification, deletion or insertion. Access control is needed to prevent unauthorized disclosure.
- The cryptographic information may be stored so as to be immediately available to an application (i.e., on a local hard disk or a server); this would be typical for keying material stored within the cryptographic module or in immediately accessible storage (e.g., on a local hard drive).
6.3.3. Periodic Key Changes at the end of the Defined Cryptoperiod

It is the policy of the Missouri Botanical Garden that keys must be changed on a periodic basis, with the frequency of key changes depending on our business needs in conjunction with our overall defensory need to protect the keys and associated system components within the cardholder data environment. During the key generation phase, the duration of the keys’ use will be determined. Additionally, when the keys are retired, they shall no longer be in use unless needed for encryption functions related to historical data recovery. For any data retention requirements for compliance, the Garden will archive the keys as necessary.

6.3.4. Retirement and Destruction of Old Keys

The end of the key life will ultimately result in key deregistration, which is the scheduled process initiated when there is no compelling business requirement (legal or compliance) for retaining the keys.

When copies of cryptographic keys are made, care should be exercised to provide for their eventual destruction. All copies of the private or symmetric keys shall be destroyed once they are no longer required (i.e., for archival or reconstruction activity) in order to minimize the risk of a compromise. Any media, upon which unencrypted keying material requiring confidentiality protection is stored, shall be erased in a manner that removes all traces of the keying material, thereby precluding its recovery by either physical or electronic means. Public keys may be retained or destroyed as desired.

6.3.5. Replacement of Known or Suspected Compromised Keys

If a key or keys have been compromised, they must expeditiously and properly be revoked in a manner that will mitigate or eliminate the impact on the cardholder environment or any supporting system components.

The process for compromised keys includes the following steps:

- Immediately remove all instances of keys that have been affected. This includes keys used in operational storage and usage.
- Immediately replace affected keys with a new set of keys that allows business operations to continue as normal.
- Lastly, if retired, replaced or compromised keys are in fact retained, they are never to be used again for encryption of cardholder data or any other operations within the cardholder data environment.

6.3.6. Prevention of Unauthorized Substitution of Keys

The substitution of keys is not permitted unless keys have been compromised, which may affect the integrity and overall security of keys utilized in conjunction with system components in the cardholder environment. Due care will be administered throughout the key-management lifecycle to ensure that the substitution of keys is prohibited. Additionally, logical and physical controls will also play a critical role in enforcing this policy.
6.4 Responsibility for Policy Maintenance

The Vice President of Information Technology is responsible for ensuring that this policy is kept current as needed for purposes of compliance with the Payment Card Industry Data Security Standards (PCI DSS) initiatives.