# Revision History

<table>
<thead>
<tr>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Publication</td>
<td>December 1, 2016</td>
</tr>
</tbody>
</table>
Table of Contents

1. INTRODUCTION AND SCOPE ............................................................................. 4
2. ROLES AND RESPONSIBILITIES ..................................................................... 4
3. ACCESS TO CARDHOLDER DATA ..................................................................... 4
4. SYSTEM COMPONENTS AND DATA RESOURCES CONTAINING CARD HOLDER DATA ............................................................................. 4
   4.1 Galaxy System ......................................................................................... 4
   4.2 Raiser's Edge System ............................................................................ 4
   4.3 Ungerboeck (EBMS) System .................................................................... 4
   4.4 Liberty system ....................................................................................... 4
5. CARD HOLDER DATA ACCESS GENERAL POLICY ..................................... 4
   • Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities................................................................. 5
   • Privileges must be assigned to individuals based on job classification and function (also called "role-based" access control)................................................................................................................................. 5
   • Require documentation approval by authorized parties specifying required privileges... 5
6. ACCESS CONTROL SYSTEM ............................................................................. 5
7. ROLES AND PRIVILEGES FOR CARD HOLDER DATA ACCESS .......... 5
   7.1 Galaxy System Roles ............................................................................. 5
   7.2 Raiser's Edge Roles ............................................................................. 5
   7.3 Ungerboeck (EBMS) Roles .................................................................... 5
   7.4 Liberty Roles ....................................................................................... 6
1. Introduction and Scope

   This document provides the Missouri Botanical Garden’s policy for access to cardholder data.

2. Roles and Responsibilities

   The Cyber Information Security Officer is responsible for compliance to this policy.

3. Access to Cardholder Data

   Access to Missouri Botanical Garden's cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

   This policy and operational procedure documents restricted access to cardholder data and must be in use and known to all affected parties. (PCI Requirement 7.3)

4. System Components and Data Resources Containing Card Holder Data

   4.1 Galaxy System

      The Galaxy System includes Point of Sale workstations, Order Entry workstations, System Administration workstations, and servers.

   4.2 Raiser's Edge System

      The Raiser's Edge System includes desktop workstations, system administration workstations and servers.

   4.3 Ungerboeck (EBMS) System

      The Ungerboeck System includes desktop workstations, System Administration workstations and servers.

   4.4 Liberty System

      The Liberty System includes Point of Sale workstations, System Administration workstations, and a server.

5. Card Holder Data Access General Policy

   - Access needs for each role must be defined including system components and data resources that each role needs to access for their job function and level of privilege required (for example, user administrator, etc.) for accessing resources
Credit Card Data Security Policies
PCI DSS 3.1 – Cardholder Data Transmission Policy

- Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities.

- Privileges must be assigned to individuals based on job classification and function (also called "role-based" access control).

- Require documentation approval by authorized parties specifying required privileges.

6. Access Control System

An access control system for system components with multiple users will be established that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following: (PCI Requirement 7.2)

- Coverage of all system components
- Assignment of privileges to individuals based on job classification and function.
- Default "deny all" setting

Galaxy, Raiser's Edge, Unberboeck (EBMS) and Liberty all utilize role-based access control systems that are set to "deny all" by default.

7. Roles and Privileges for Card Holder Data Access

7.1 Galaxy System Roles

1. System Administrator – requires access to all system components and servers
2. Supervisor – requires access to user administration software components, tickets creation and administration, credit card transaction records, and system reports.
3. User – requires access to sell tickets and other items from one point of sale or workstation.

7.2 Raiser's Edge Roles

1. System Administrator– requires access to all system components and servers
2. Supervisor - requires access to user administration software components, constituent administration, credit card transaction records, and system reports.
3. User – requires access to record and update constituent information.

7.3 Ungerboeck (EBMS) Roles

1. System Administrator– requires access to all system components and servers
2. Supervisor - requires access to user administration software components, schedules and facilities administration, credit card transaction records, and system reports.
3. User - requires access to record and update schedule and facility information.
7.4 Liberty Roles

1. System Administrator – requires access to all system components and servers
2. Supervisor - requires access to user administration software components, PLU creation and administration, credit card transaction records, and system reports.
3. User - requires access to sell PLUs from one point of sale or workstation.