# Authentication Methods Policy

## Overview

In accordance with the Payment Card Industry Data Security Standards (PCI DSS) requirements, the Office of Information Security has established a formal policy and supporting procedures concerning other various authentication methods, such as shared, group, generic, and any other specific methods. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

## Policy

The Office of Information Security will ensure that the Shared, Group, Generic, and Other Authentication Methods 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):

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that Generic user IDs are disabled or removed.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that shared user IDs for system administration activities and other critical functions do not exist.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that shared and generic user IDs are not used to administer any system components.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited.
- Ensure that system administrators understand that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested.

- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that different authentication is used for access to each customer.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that procedures for using authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include authentication mechanisms that are assigned to an individual account and not shared among multiple accounts and that physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access.
- Appropriately configure, examine, and confirm system settings and all necessary configurations for system components to ensure that controls are implemented to ensure only the intended account can use that mechanism to gain access.

## Responsibility for Policy Maintenance

The Office of Information Security 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.

## Revision History

February 8, 2019 (Policy Created)

July 15, 2019 (Policy Modified)

Adapted from Stanford University's PCI DSS Policies 1-2019