Unique ID & 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 unique ID and authentication 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 Unique ID and 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):

- All users are assigned a unique ID before allowing them to access system components or cardholder data.
- Authorized personnel are to control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
- Terminated users are to have their access immediately revoked.
- Inactive user accounts are to be disabled and/or removed every 90 days.
- Authorized personnel are to manage IDs used by vendors to access, support, or maintain system components via remote access as follows:
    - Enable vendor access only during the time period needed and disabled when not in use.
    - Actively monitored when in use by all appropriate means.
- Additionally, the following best practices are to be implemented regarding accepts attempts and system idle time:

  - Limit repeated access attempts by locking out the user ID after not more than five attempts.
  - Set the lockout duration to require an administrator re-enable the user ID.
  - If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

- Additionally, all users are to be assigned a unique ID for access to system components or cardholder data and must also utilize an approved authentication method.
- Passwords/phrases must meet the following conditions in accordance with PCI DSS mandates as described in the Password Policy.

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