Unencrypted Primary Account Numbers (PAN) 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 unencrypted Primary Account Numbers (PAN) that are not to be sent via end-user messaging technologies. This policy is to be implemented immediately. It will be evaluated on an annual basis to ensure its adequacy and relevance.

Policy

Office of Information Security will ensure that unencrypted Primary Account Numbers (PAN) are not sent via end-user messaging technologies and that they adhere 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):

- Primary Account Numbers (PAN) will not be sent via email.
- Primary Account Numbers (PAN) will not be sent via an instant messaging protocol.
- Primary Account Numbers (PAN) will not be sent via a chat protocol or forum sessions.
- If for any reason, Primary Account Numbers (PAN) must be sent via end-user messaging technologies, they are to be sent using strong encryption, rendering the PAN unreadable.

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