# Changing of Vendor Supplied Default Settings 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 for the changing of vendor supplied default settings for all system components. 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 changing of vendor default settings for all system components and wireless environments 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):

- Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. Note: This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.). (Req. 2.1).

- All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are to be changed before a system is installed on the network. (Req. 2.1.c).

- Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are to be removed or disabled before a system is installed on the network. (Req. 2.1.c).

- Appropriately configure, examine, and confirm system settings and all necessary configurations to ensure that encryption keys are changed from default at installation. (Req. 2.1.1.a).
- Appropriately configure, examine, and confirm system settings and all necessary configurations to ensure that default SNMP community strings are changed upon installation. (Req. 2.1.1.b).
- Appropriately configure, examine, and confirm system settings and all necessary configurations to ensure that default SNMP community strings are not used. (Req. 2.1.1.c).

## 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