# Personal Firewall 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 personal firewall software on any mobile computers. 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 personal firewall on any computers in the PCI environment 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):

- Personal firewall is required for all devices that connect to the Internet (for example, laptops used by employees) when outside the company network, and which are also used to access the company network. (Req. 1.4).
- Specific configuration settings are defined for personal firewall. (Req. 1.4).
- Personal firewall software is to be configured to actively run on all such devices that are used within the PCI environment. (Req. 1.4).
- Personal firewall software is to be configured in such a way that is not alterable by users of any device. (Req. 1.4).

## 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