PCI Network - User Accounts Procedure

Office: Information Technology
Procedure Contact: IT Infrastructure Manager
Related Policy or Policies: PCI Network - Device Security, PCI Network - Network Security

Revision History

Revision Number:	Change:	Date:
1.1	Formatting modification and expansion of Sections B, C	**June 2017**
1.0	Initial Version	**May 2017**

A. Purpose

User accounts with access to networks within the scope of PCI compliance must adhere to elevated security standards to prevent unauthorized access to sensitive data.

B. Definitions

"PCI" stands for "Payment Card Industry".

"DSS" stands for "Data Security Standards".

“User” shall refer to a single person with access to devices and/or network resources.

A “network” is a system of electronic devices interconnected by telecommunication equipment or cables used to transmit or receive information. The bounds of a “network” may be defined by the ability of traffic to pass unimpeded between devices, similar to a broadcast domain, or a specific range of IP addresses, around which connectivity restrictions are based.

A "PCI network" refers to any network as defined above, intended to enable credit card processing.

A “device” is a unit of physical microprocessor equipment, that either resides on a PCI network, or has direct access to the data/traffic on the PCI network.

"CDE" stands for "Cardholder Data Environment". The CDE is the the networks and devices involved in processing credit card transactions.

A “firewall” may be a device as defined above, or a software application, with the capability and intended purpose of filtering traffic in and/or out of a network.

Accessing a device “remotely” refers to any non-console access, or any console access that does not require physical presence at the device.

C. Procedures

In addition to the policies and procedures stated in the SOU Account Policy, and the SOU Computing Resources Acceptable Use Policy, accounts for users with access to resources on PCI networks must also adhere to the standards below:

1. A user’s account will not be authorized to access the CDE until the user has undergone training for PCI security, covering the materials contained within this document and PCI Network - Device Security.
2. All user accounts will be password protected
3. All user account passwords will meet the following requirements:

   a. Minimum password length of 8 characters, containing both numeric and alphabetic characters
   b. Passwords will be changed every 365 days
   c. New passwords must be different from any of the user's last four passwords
   d. If a password is reset for a user (meaning the user did not initiate the password change themselves) the user must change their password immediately after the first use.

4. The list of users allowed to access PCI resources electronically will be audited quarterly and any discrepancies will be remedied and documented in the department ticketing system.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately upon approval.