THE UNIVERSITY OF UTAH

Version:	Modified By:	Date:	Approved By:	Date:
1.0	Lisa Zaelit	February 7, 2014	Dan Bowden	February 28, 2014
2.0	Kim Stringham	August 12, 2015	Lisa Zaelit	August 20, 2015
3.0	Stu Schrager	May 14, 2018	Lisa Zaelit	May 16, 2018

DEPARTMENT PROCEDURE FOR STANDARD 9 – Restrict Physical Access to Cardholder Data

Purpose

The purpose for restricting physical access to cardholder data is to ensure that unauthorized persons are prevented from having access to cardholder data.

Procedure

A. **Physical Access Restriction -** Standard 9.6:

1. All cardholder data shall be kept physically secure.
    a. Cardholder data, either on paper or electronic media, when not in use, needs to be kept secure, in a locked filing cabinet, within a locked room, with limited access to designated personnel only, in a room with either a security camera with 3 months legacy data, or an electronic key or card entry.
2. Controls should be in place to limit access to designated personnel needing access to the cardholder data to do their job.

B. **Maintain Strict Control over Media –** Standard 9.9:

1. All paper and electronic media should have controls in place for storage and accessibility.
    a. Only personnel with a need for this information should be able to access these areas.
    b. A log should be maintained of what and when this media was stored, and who is accessing it.
        i. A name, date, and reason for access should be entered into the log.
        ii. Confirmation of what is being stored, and what is on the log, should be compared twice a year.

C. **Media Needs to be Destroyed or Made Unrecoverable -** Standard 9.10:

1. Paper and electronic media should be destroyed either after a period of time, or when it is no longer needed.
    a. Cardholder data on a paper media shall be destroyed within 24 hours by crosscut shredding.

    i. If cardholder data to be destroyed is stored in a container to be shredded, it should be locked.
    ii. Two people need to confirm and document that cardholder data is picked up and destroyed.

b. Cardholder data on electronic media should be rendered unrecoverable, and cannot be reconstructed.

    i. A secure wipe program can be used, or it should be physically destroyed.