Policy: 01-12-02

Credit Cardholder Data Access Control in Compliance with Payment Card Industry Data Security Standards (PCI DSS)

OFFICE OF RECORD: Business Office
ISSUED BY: Vice President for Business Affairs
APPROVED BY: *Douglas D. Knowlton, Pres*
EFFECTIVE DATE: 11/01/2010

Purpose

In accordance with Payment Card Industry Data Security Standards (PCI DSS) requirements, Dakota State University has established a formal policy and supporting procedures regarding cardholder data access control. This policy will be evaluated on an annual basis.

Scope

This policy applies to all systems in the cardholder data environment. For definitions of certain terms, see the Compliance with Payment Card Industry Data Security Standards (PCI DSS) policy document.

Policy

Dakota State University will protect cardholder data by ensuring the following access controls are in place in the cardholder data environment:

- Access rights for privileged users are restricted to the fewest privileges necessary to perform job responsibilities
- Privileges are assigned to individuals based on job classification and function, such as Role-Based Access Control (RBAC)
- An e-mail process is utilized to request access to cardholder. This request must specify the privileges requested and the duration of the request. The

message must be submitted to the Network Security Officer by the individual's supervisor.

- Access controls are implemented via an automated access control system
- Access control systems are in place on all system components
- Access control systems are configured to enforce privileges assigned to individuals based on job classification and function
- Access control systems have a deny all setting