Policy: 01-12-05

Information Security Responsibilities Related to 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 Information Security Responsibilities. This policy will be evaluated on an annual basis.

Scope

This policy applies to all employees and contractors who have access to the DSU cardholder data environment. For definitions of certain terms appearing in italics, see the Compliance with Payment Card Industry Data Security Standards (PCI DSS) policy document.

Policy

DSU will ensure that the Information Security Responsibilities policy adheres to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council 2009):

- Formal assignment of information security is to be given to the DSU CIO and Director of Computing Services.

- The responsibility for creating and distributing security policies and procedures is to be formally assigned to the CIO and Director of Computing Services.
- The responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is to be formally assigned to supervisor of the DSU Network and Security Group within Computing Services.
- The responsibility for creating and distributing security incident response and escalation procedures is to be formally assigned to the supervisor of the DSU Network and Security Group within Computing Services.
- The responsibility for administering user account and authentication management is to be formally assigned to the supervisor of the DSU Network and Security Group within Computing Services.
- The responsibility for monitoring and controlling all access to cardholder data is to be formally assigned to the Controller.