Policy: 01-12-04

Use of Employee Facing Technologies 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 the use of employee facing technologies. This policy will be evaluated on an annual basis.

Scope

This policy applies to all Dakota State University employee facing mobile technology used in the cardholder data environment. Employee facing mobile technologies are system components and additional IT resources deemed critical by Dakota State University. Some examples of employee facing technologies are:

- Remote access technologies
- Wireless technologies
- Removable electronic media
- Laptops
- Personal Data Assistants (PDA)
- Cell phone

For definitions of certain terms see the Compliance with Payment Card Industry Data Security Standards (PCI DSS) policy document.

Policy

Dakota State University will ensure that the usage policies for critical employee facing technologies will adhere to the following conditions for purposes of complying with the Payment Card Industry Data Security Standards (PCI DSS) initiatives (Security Standards Council 2009):

- DSU will require explicit management approval to use the technologies.
- DSU will require all technology use be authenticated with user ID and password or other authentication item.
- DSU maintains a list of all devices.
- DSU will require acceptable uses for the technology.
- DSU will require acceptable network locations for the technology.
- DSU will require a list of company-approved products.
- DSU will require automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.
- DSU will require activation of remote-access technologies used by vendors only when needed by vendors, with immediate deactivation after use.
- DSU will prohibit copying, moving or storage of cardholder data onto local hard drives or removable electronic media when accessing such data via remote-access technologies.