UNIVERSITY OF SOUTH DAKOTA

Policy Number:	5.003
Originating Office:	Information Technology Services
Responsible Executive:	Vice President for Administration and Technology
Date Issued:	12/08/2010
Date Last Revised:	12/10/2012

Information Security Responsibilities

Policy Contents

I. REASON FOR THIS POLICY

The university is required to protect its information technology resources, comply with applicable laws and regulations, and comply with South Dakota Board of Regents policy for the protection and preservation of data. This includes compliance with Payment Card Industry Data Security Standards (PCI-DSS). This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding The University of South Dakota's needs and goals.

Policy last reviewed 8/5/15 by CIO Management Team

II. STATEMENT OF POLICY

USD employees are required to be responsible users of university information technology resources and to take appropriate measures to manage the security of those resources, and the data therein, by understanding and complying with policies, requirements and best practices.

III. DEFINITIONS

PCI Employee facing technologies: System components and additional I.T. resources deemed critical by USD. Employee facing technologies include, but are not limited to, desktop and laptop computers used to enter cardholder data, and Point of Sale (POS) terminals.

IV. PROCEDURES

User Responsibilities

1. Understand and comply with current policies, requirements, guidelines, procedures, and protocols concerning the security of the university's electronic resources.
2. Ensure that personally identifiable information (credit numbers, SSN, etc.) is not sent unencrypted over email, instant messaging, chat, forums or any other end-user messaging technologies.
3. Enter cardholder data only on PCI employee facing technologies that are properly installed in the appropriate network location.
4. Comply with guidelines and practices established by USD ITS.
5. Contact the ITS Help Desk whenever a questionable situation arises regarding the security of your IT device(s).
6. Reports all electronic security incidents to the Help Desk immediately.
7. All USD-owned laptops will be encrypted by ITS using standard drive encryption software to prevent unauthorized access in the event the laptop is lost or stolen.

ITS Security Officer Responsibilities

1. Develop a comprehensive security program that includes risk assessment, best practices and education.
2. Create and distribute security incident response and escalation procedures.
3. Assist or lead electronic security incident resolution for the university and individual units.
4. Develop, implement, and support security monitoring and analysis.
5. Monitor and analyze security alerts and distribute information to appropriate management personnel.
6. Support and verify compliance with federal, state, and local legislation as well as industry standards including Payment Card Industry Data Security Standards (PCI-DSS).

Desktop Technician Responsibilities

1. Be knowledgeable and comply with current policies and procedures concerning the security of the university's information technology resources.
2. Understand and document the specific configurations and characteristics of the IT devices he or she supports to be able to respond to emerging technology threats and to support security event mitigation efforts.

3. Understand and recommend appropriate measures to provide security to resources under his or her control. These include:
    a. Most recently tested and approved software patches available
    b. Most current and available security configurations
    c. Most recent and available virus protection
    d. Configuration of secure passwords on all IT devices, changing all default or administrative passwords.
4. Ensure that PCI employee facing technologies are installed in the correct network location.

Information Services and Server Team Responsibilities

1. Ensure that all systems containing sensitive user information is not available in clear text.
2. Ensure that PCI employee facing technologies are installed in the correct network location.

V. RELATED DOCUMENTS, FORMS AND TOOLS

Incident Handling Policy 5.004

Board of Regents Acceptable Use of Information Systems Policy 7:1 - https://www.sdbor.edu/policy/documents/7-1.pdf