SONORAN UNIVERSITY
OF HEALTH SCIENCES

Data Protection/Authorization Standards Policy

Policy Number:
Owner Department: Information Technology Department
Approved/Effective Date: February 24, 2011
Approved By**:** President's Council

I. POLICY STATEMENT/PURPOSE

Sonoran University requires sufficient data and network access controls to protect confidential and personal electronic information. The purpose of the Authorization Standard is to provide guidance to those who are responsible for granting access to Sonoran University's technology resources and data. The technology resources and data referred to in this standard include those owned by or entrusted to the university for the purpose of supporting academic, administrative, research or service-related activities.

In addition to fulfilling the responsibility of effectively protecting data belonging to the university, as well as its customers and partners, the university must implement appropriate controls to help ensure compliance with external regulations, including but not limited to:

1. Family Educational Rights & Privacy Act (FERPA)
2. The Health Insurance Portability and Accountability Act (HIPAA)
3. Payment Card Industry Data Security Standard (PCIDSS)
4. Social Security Numbers (SSN)
5. Employee Personnel Records

II. POLICY STATUS

New

III. HISTORY/BACKGROUND

N/A

IV. DEFINITION(S)

N/A

V. SCOPE/KEY STAKEHOLDERS

Stakeholders are defined as Sonoran University network users: Faculty, staff, and students, contractors, consultants, vendors and all others granted use of or access to Sonoran University data and technology resources.

VI. POLICY ITEMS

A. Sonoran University entities with ownership and custodial responsibility for operating and maintaining university applications/systems and data must implement formal procedures for granting, tracking and revoking access to data. With respect to technology resources, this authorization is typically implemented through the assignment of an electronic account, access card or other authentication mechanism. Authorization must be based on the least privilege and need to know principles according to an individual's job responsibilities. The authorization controls must include methods to collect and maintain the following records:
    a. Purpose for access to the resource or data
    b. Dates of authorization (initial and subsequent changes)
    c. Effective dates or duration of authorization
    d. Record of individual(s) authorizing the access
    e. Record of the individual(s) receiving the access privileges
    f. Type and scope of access privileges
    g. Procedures for tracking accounts and privileges based on responsibilities and employment status, including position changes or separation from the University

VII. RESPONSIBILITY FOR IMPLEMENTATION

All members of the Sonoran University community are responsible for information security. The IT department's Network Administrator is responsible for ensuring proper security controls are implemented.

VIII. RELATED POLICIES

IT Acceptable Use Policy

IX. RELATED DOCUMENTS

New User Request Form

X. NEXT REVIEW DATE

As needed

XI. VERSION CONTROL AND CHANGE HISTORY

Version Control	Approved By/Date	Date Effective	Amendment
1	President's Council/ February 23, 2011	February 24, 2011	
2			

XII. POLICY AUTHOR/CONTACT

Paul Collins – Senior Director of IT