SONORAN UNIVERSITY
OF HEALTH SCIENCES

I.T. Password Security Policy

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

I. POLICY STATEMENT/PURPOSE

Passwords are an important aspect of computer security. They are the front line of protection for user accounts and sensitive data. A poorly chosen password may result in the compromise of Sonoran University’s entire network. As such, all employees, faculty, and students (including contractors and vendors with access to Sonoran University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords. The purpose of this policy is to provide guidance for the proper use of passwords at Sonoran University and to establish a standard for creation of strong passwords, the protection of those passwords and the frequency of change.

II. POLICY STATUS

New

III. HISTORY/BACKGROUND

N/A

IV. DEFINITION(S)

N/A

V. SCOPE/KEY STAKEHOLDERS

The scope of this policy includes all personnel and students who have or are responsible for a network account (or any form of access that supports or requires a password) on any system that resides at any Sonoran University facility, has access to the Sonoran University network, or stores any non-public Sonoran University information. All user-level and system-level passwords must conform to the guidelines described below.

Stakeholders are defined as Sonoran University computer network users: Students, Faculty and Staff.

A. Exemptions:

a. Due to the nature, scope, and responsibilities inherent to the Information Technology department's duties, certain elements of this policy are exempt for IT personnel.

b. General purpose user-specific accounts/user ID's established for internal use such as: Student, Biopac and Medicinary are exempt from certain elements of this policy.

c. Student and Alumni accounts established for the sole purpose of email communication are exempt from this policy.

d. Application-specific accounts/user ID's established for support purposes are exempt from this policy.

e. Equipment which requires static user ID's and passwords such as surveillance cameras, loaner laptops and network monitoring applications are exempt from this policy.

VI. POLICY ITEMS

A. The university uses passwords for various purposes that include but are not limited to: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and enterprise applications storing sensitive or personal information. Few systems support one-time passwords (i.e. dynamic passwords which are only used once), thus everyone should be aware of how to select strong passwords.

a. Network login policy requires that passwords be changed at least every 90 days.
b. Network login policy requires that all passwords have at least seven (7) characters.
c. Network login and ancillary applications requiring separate passwords checks the length of passwords automatically at the time that users construct or select them.
d. After ten (10) unsuccessful attempts to enter a password, each system will suspend the involved user- ID until reset by a system administrator.
e. The previous seven (7) passwords cannot be reused.
f. The minimum period a password can be used before changing is 15 days.

B. User accounts that have system-level privileges granted through group memberships or applications should have a unique password from all other accounts held by that user unless single-sign-on is activated by the IT department.

C. Application-specific user ID's are not configurable to comply with network password configuration rules and thus cannot be enforced with centralized administration. Users are encouraged to change application-based passwords on a regular basis. All other user responsibilities and aspects of this policy pertain to application specific user ID's.

D. System and application administrators will ensure that vendor supplied accounts are secure. Such account should be enabled only when necessary for vendor access. This applies to operating system and application software.

E. The Information Technology department does not solicit nor require users to provide password information. Personnel must never respond to email or telephone queries with password or personal information

F. Enforcement

   a. Since password security is critical to the security of the organization and everyone, employees who do not adhere to this policy may be subject to disciplinary action up to and including dismissal.

VII. RESPONSIBILITY FOR IMPLEMENTATION

Network Administrator

VIII. RELATED POLICIES

IT Acceptable Use Policy

IX. RELATED DOCUMENTS

Form: IT New Hire Checklist

Procedure: Password Guidelines

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