SIU CARBONDALE SOUTHERN ILLINOIS UNIVERSITY OFFICE OF INFORMATION TECHNOLOGY

Password/Passphrase Standard

Document Number:	ISP-005	**Version:**	1.3
Document Owner:	Director of Information Security	**Effective Date:**	09/01/2014
Responsible Office:	Office of Information Technology	**Last Update:**	04/14/2022

TABLE OF CONTENTS

PURPOSE

[TOP]

The purpose of this standard is to establish a set of requirements for the creation of strong passwords/passphrases, the protection of those passwords/passphrases, and the frequency of change.

SCOPE

[TOP]

The scope of this standard includes all Southern Illinois University (SIU) affiliated personnel (See Roles & Responsibilities) who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Southern Illinois University facility, has access to the Southern Illinois University network, or stores any non-public Southern Illinois University information. Some exceptions may apply. Contact the Information Security Team (security@siu.edu) with questions and for clarification.

STANDARD [TOP]

The following minimal password/passphrase requirements must be followed:

A. All system-level passwords/passphrases (e.g., root, Windows Server Administrator, application administration accounts, etc.) must be changed at least every 180 days.

B. All user-level passwords/passphrases (e.g., email, web, desktop computer, etc.) must be changed at least every 365 days.

C. All user-level and system-level passwords/passphrases must conform to the requirements described below.

PASSWORD/PASSPHRASE CONSTRUCTION

The following are password/passphrase requirements that all SIU users must adhere to when changing their password/passphrase. Minimally, the password/passphrase:

- Cannot be reused in the case of a password reset (i.e., Network ID)
- Must be at least 16 characters in length (max 30 characters for AIS and Banner)
- Must contain one or more of these special characters: **{}[]!+-_~?.**
- May include spaces (Banner does not support).
- May include upper case and lower-case letters.
- May include numbers.
- May be in the form of a passphrase (e.g., "Two + 2 makes four!").
- Cannot contain your name or username (Network ID).
- Cannot contain restricted dictionary words as determined by the Identity and Access Management (IAM) system (applies to Network ID password/passphrase).

In addition, the password/passphrase:

- Should not be a common phrase (e.g., “an arm and a leg” or “between a rock and a hard place”).
- Should not be based on predictable patterns (e.g., “abcdefg” or “123456”).
- Is case sensitive. For example:
    - The lowercase c is a different letter from the uppercase C . Make sure that the Caps Lock key is not on when creating a password/passphrase.
- Passphrases are recommended as a secure alternative to password creation. The use of distinguishing words, separated by one or more non letters (space may not be supported in some systems), can be a good practice. For example:

- "will_be+Saluki4life" contains four "words" and would therefore be a valid passphrase.

PASSWORD/PASSPHRASE PROTECTION

- Always use different passwords/passphrases for SIU accounts from other non-SIU accounts (e.g., banking, social media, etc.).
- Do not share SIU passwords/passphrases with any unauthorized, including administrative assistants or other supporting staff.
- All passwords/passphrases are to be treated as sensitive, confidential SIU information.
- Passwords/passphrases should never be written down or stored on-line without encryption.
- Do not reveal a password/passphrase in email, chat, or other electronic communication.
- Do not discuss a password/passphrase in front of others.
- Do not hint at the format of a password/passphrase (e.g., "pet name")
- Do not reveal a password/passphrase on questionnaires or security forms
- If someone demands a password, refer them to this document and direct them to the Information Security Team.
- It is good practice to always decline the use of the "Remember Password" feature of applications (e.g., web browsers, email, etc.).

If an account or password/passphrase compromise is suspected, report the incident to the Information Security Team (security@siu.edu) immediately.

APPLICATION ADMINISTRATION

Application administrators must ensure their systems contain the following security precautions. Applications:

- Shall support authentication of individual users, not group accounts (accounts shared by more than one user).
- Shall not store passwords/passphrases in clear text or in any easily reversible form unless otherwise not supported by the application.
- Shall provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

MULTI-FACTOR AUTHENTICATION (MFA)

Some accounts may require the addition of multi-factor authentication to be used in conjunction with the password/passphrase to access resources. For details refer to the: Identity and Access Standard and Identity and Access Procedures.

ROLES AND RESPONSIBILITIES [TOP]

All SIU personnel including, but not necessarily limited to, faculty, staff, Civil Service, Administrative Professional, outsourced contractual workers, guests, volunteers, temporary extra help, student workers, graduate assistants, and undergraduate assistants are required to abide by the requirements and standards established within this standard.

DEFINITIONS [TOP]

Application – Applications sit atop systems software and require the services of the computer's operating system, system utilities, and other supporting applications to operate. For the purposes of this standard, application generally refers to AIS and Banner, including the underlying Oracle databases, as well any other enterprise level application in support of SIU business processes.

Application Administration Account - Any account that is for the administration of an application.

Network ID - Network IDs are used to manage access to network-based resources (e.g., Morris Library and Computer Learning Center facilities, campus network, SalukiNet, electronic mail,

wireless access, the campus single sign on environment, etc.). This consolidated approach to network identification provides users with the ability to use the same ID and password/passphrase for all services. Thus, a change in a user's Network ID password/passphrase affects access to all these services.

Passwords - Passwords are short sequences of letters, numbers, and symbols that are entered to verify the user's identity to a system, which then allows access to secure data or other resources. The role of a password is to prevent unauthorized access to data just as a key prevents unauthorized access to a house or apartment.

Passphrases - Passphrases operate on the same principle as passwords and are used in the same way. However, they differ from traditional passwords in two aspects:

- Passphrases are generally longer than passwords. While passwords can frequently be as short as six or even four characters, passphrases have larger minimum lengths and, in practice, typical passphrases might be 16 or 30 characters long or longer. This greater length provides more powerful security; it is far more difficult for security attacks against passwords to break a 16-character passphrase than an eight-character password.
- The rules for valid passphrases differ from those for passwords. Systems that use shorter passwords often disallow actual words or names, which are notoriously insecure; instead, your password is usually an apparently random sequence of characters. The greater length of passphrases, by contrast, allows you to create an easily memorable phrase rather than a cryptic series of letters, numbers, and symbols.

COMPLIANCE

[TOP]

Violations of this Standard may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and University owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the University. Civil, criminal, and equitable remedies may apply.

REFERENCES

[TOP]

NIST SP 800-118
ISP-015 Identity and Access Standard
ISP-016 Identity and Access Procedures

AUTHORITY [TOP]

Southern Illinois University Board of Trustees Policy, SIU System Information Security Plan.
Southern Illinois University Carbondale Information Security Program (ISP).

REVISION HISTORY [TOP]

Version	Description	Revision Date	Reviewed By
1.0	Standard was approved by CIO.	09/01/2014	Director of Information Security
1.1	Reviewed. Fixed broken links.	06/24/2019	Director of Information Security
1.2	Reviewed. Updated Links. Added restricted dictionary word requirement.	02/26/2020	Director of Information Security
1.2	Reviewed. Updated Links. Adjusted password/passphrase construction section to formatting and flow.	03/30/2021	Director of Information Security
1.3	Reviewed. Updated links. Added MFA reference and provided links to IAM standards and procedures.	04/05/2021	Director of Information Security
1.3	Reviewed, minor grammatical updates only, no content changes.	04/14/2022	Acting Director of Information Security and Associate Director, PMO