

1. Overview

Password/passphrases are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password/passphrase may result in the compromise of individual systems, data or the entire University of Arizona network. All University of Arizona affiliates, including contractors and vendors, with access to University resources are responsible for taking the appropriate steps, as outlined below, to construct and maintain secure password/passphrases.

2. Purpose

The purpose of this document is to establish a guideline for password/passphrase construction, protection and expiration.

3. Scope

This guideline applies to all University of Arizona affiliates with access to any resource that supports or requires a password/passphrase. Specifically this guideline applies to all resources residing at any university facility; having access to the university network; or storage of any university information. This is a minimum guideline, and departments are encouraged to maintain stricter limits.

4. Standards

All university-affiliated password/passphrases should meet or exceed the guidelines described below.

4.1. Construction

One of the first things an attacker may do is run a program that attempts to guess the password/passphrase of the target. These programs contain entire dictionaries of several languages. In addition to containing dictionary word lists, they frequently create words and contain word lists from popular culture, such as slang terms, movies, novels, etc.

Users should construct a password/passphrase that meets the minimum following criteria:

Password/passphrases should ALWAYS contain:

- At least eight characters (but more is highly recommended)
- Both upper and lower case letters

- At least one number
- At least one special character (e.g., !@\$%^&*()_+|~-=\`{}[]:"';<>?,./)

Password/passphrases should NOT:

- Be based on personal information, such as names of family, dates, addresses, phone numbers, etc.
- Be based on work information, such as room numbers, building name, co-worker's name, phone number, etc.
- Use word or number patterns like, aaabbb, qwerty, zyxwvuts, 123321, abcABC123, etc.
- Be a word found in any dictionary in any language, slang, dialect, jargon, etc.
- Be based on your username, your real name, handle, nickname, screen name, etc.

The following section describes how to create a password/passphrase which includes all aspects of the criteria above making it hard to guess yet easy to remember. Be aware that some systems do not allow password/passphrases to meet all of the above criteria – for password/passphrase construction on such systems, follow all possible recommendations and contact your system administrator for suggestions on compensating for these limitations.

One way to meet the suggested criteria is to mix special characters, upper and lowercase letters, and numbers, and associate them with a phrase or song titles. The following examples demonstrate how you might do this.

Example I:

Step 1 – Choose a Phrase: *Home of the University of Arizona Wildcats*

Step 2 – Use the first character of each word: *HotUoAW-c*

Note: to meet the eight-character minimum, we hyphenated “Wildcats” as W-c

Step 3 – Substitute special characters and numbers to increase complexity:
H0tUo@UU-c!

Note: choose substitutions that are meaningful to you, to make it easier to remember

Step 4 – Review your password/passphrase to ensure that it meets all of the above requirements.

Example II:

Step 1 – Choose a Phrase: *Why did the chicken cross the road?*

Step 2 – Use the first character of each word: *Wdtcctr?*

Step 3 – Substitute special characters and numbers to increase complexity:
Y?d7CxtR?

Note: choose substitutions that are meaningful to you, to make it easier to remember

Step 4 – Review your password/passphrase to ensure that it meets all of the above requirements.

Example III (BEST OPTION if system allows for more characters):

Step 1 – Choose and Use a Phrase or Sentence: *Why did the chicken cross the road?*

Step 2 – Include numeric and special characters in the passphrase: *Why did the 3 chickens cross the road?*

Step 3 – Review your password/passphrase to ensure that it meets all of the above requirements.

You can make strong password/passphrases by simply substituting numbers for letters or words (or vice versa). Such as: E equals 3, I equals 1, O equals 0 (zero), for equals 4, two equals 2, B equals 8, see or sea equals C, etc. Additionally, you should add a special character in the middle. The best password/passphrases are created using an easy to remember phrase as outlined in the above table. More examples of strong password/passphrases follow:

- **My four children are wonderful when they're sleeping** m4caW,wtS
- **My anniversary is April 4 remember that date** Maia4,rtd
- **Ali Baba had forty thieves** @Bh?4tyt
- **Wildthing** W!ld*7H1ng

OR

- **Use R3d-j3llo instead of redjello (substitute the E's with 3's)**
- **Use B,c11nt0n instead of bclinton (substitute I & L with 1's and O with zero)**
- **Use J0hn(80y) instead of johnboy (substitute the O's with zeros & the B with 8)**

NOTE: Never use published example password/passphrases such as the ones above.

4.2. Protection

Password/passphrases are an important tool available to users to protect resources. Unfortunately, people are not accustomed to memorizing difficult password/passphrases that include numbers and special characters. This is made more difficult due to the ever-increasing number of password/passphrases required in today's world. Many people have chosen to write down their password/passphrases and keep them in an unsecured area, such as under their keyboard, filed in a rolodex, or posted on their computer screen. All users should use the following security measures to protect their password/passphrases and associated accounts:

- Password/passphrases should be memorized and not written down or stored on-line. If you must write down a password/passphrase it must be stored in a secure location allowing only authorized access, such as a locked filing cabinet or safe.
- Password/passphrases assigned to individuals should not be shared with anyone, even your supervisor. All password/passphrases must be treated as sensitive/confidential information.
- Anyone requesting an individual's password/passphrase should be referred to the Information Security Office and this guideline.
- Password/passphrases should not be included in email messages or other forms of electronic communication such as instant messengers, chat rooms, and wireless text messaging, etc.
- User accounts that have system-level privileges granted through group memberships or programs (such as the "Administrators" group in Windows or "sudo" in Unix) should have a different password/passphrase than all other accounts held by that user.
- Never use a university password/passphrase when joining internet sites, such as eBay, Yahoo, Hotmail, Amazon, etc.
- All accounts used for business or financial transactions should use a unique password/passphrase.
- Don't talk about a password/passphrase in front of others or reveal a password/passphrase over the phone.
- All default password/passphrases must be changed as soon as possible.

4.3. Maintenance

It is important to remember that given enough time, any password/passphrase can be guessed using currently available software; therefore, it is critical that password/passphrases be changed regularly based on complexity rules. Users should not reuse any recent password/passphrases when creating a new password/passphrase. The recommended password/passphrase change interval is every 180 days when constructing a password/passphrase following the minimum recommendations in this guideline.

4.4. General

If you suspect that an account or password/passphrase has been compromised, change the password/passphrase or disable the account immediately, then contact your system administrator or refer to the Incident Handling Standard.

Additional recommended password/passphrase security measures:

- Do not use the same password/passphrase for University of Arizona accounts as for other non- University of Arizona access (e.g., personal Internet account, option trading, benefits, etc.).
- Where possible, don't use the same password/passphrase for various University of Arizona access needs. For example, select one password/passphrase for your NetID account and a separate password/passphrase for your departmental account. Ideally, you should have different password/passphrases for different systems, such as FRS or PSOS.
- Do not use the "Remember Password/passphrase" feature in applications such as Eudora, Outlook, and Netscape Messenger.
- Never provide any current password/passphrase or variation of it to an internet site that requests your email address and then requests a password/passphrase.
- If exceptional circumstances require you to disclose a password/passphrase, the password/passphrase should be changed as soon as possible.

5. Enforcement

Password/passphrase cracking or guessing may be performed on a periodic or random basis by ISO or its delegates. If a password/passphrase, not meeting these standards is guessed or cracked during one of these scans, the user will be required to change it.

If a password/passphrase is revealed to have been compromised the user will be required to change it.

Any employee found to have violated this standard may be subject to disciplinary action, up to and including termination of employment.

Related Guidance

Information Security Terms Guideline (IS-G100)
Standards, Procedures and Guidelines at <http://security.arizona.edu>

All italicized terms used in this standard are defined in the Information Security Terms Guideline.

Revision History

Initial Draft	5/25/06
Effective Date	5/27/08