

*Best Security Practice for*  
**PASSWORD STANDARDS for PERSONAL SYSTEMS**  
**(with GUIDELINES)**

*PUBLISHED BY THE OFFICE OF INFORMATION TECHNOLOGY – CANUARY 2008*

*"BEST PRACTICES ARE THE PROCESSES AND ACTIVITIES THAT HAVE BEEN SHOWN TO BE THE MOST EFFECTIVE"*

---

**BEST SECURITY PRACTICE (BSP) No. 1:** ALL UNLV COMPUTERS SHOULD EMPLOY PASSWORDS OF AT LEAST 10 CHARACTERS. COMPUTING SYSTEMS INCAPABLE OF EMPLOYING 10 CHARACTER PASSWORDS SHOULD USE THE MAXIMUM SIZE ALLOWABLE BY THE SYSTEM(S). PASSWORDS SHOULD BE CREATED/SELECTED USING THE GUIDELINES OUTLINED BELOW.

---

**OBJECTIVES:** To provide direction and support for information security in accordance with internationally accepted standards (ISO 17799/27001), business requirements and relevant State and Federal laws and regulations. This technical Best Practice directly supports the UNLV Capstone Policy IS01 - Information Security for Information Resources and Asset, and defines the acceptable use of UNLV information technology services and accounts. **This BSP is the foundation for the forthcoming UNLV Password Standard Policy (IST102).**

**BACKGROUND:** Passwords are an important aspect of computer security. They are the first line of protection for access to user accounts and contribute to the baseline security structure for a defense-in-depth integrated security. A poorly chosen password may result in the compromise of UNLV's entire campus network. As such, all UNLV students and employees (including contractors and vendors with access to UNLV systems) are responsible for taking the appropriate steps, as outlined below, to create/select and secure their appropriate passwords.

The purpose of this Practice is to:

- Ensure that access to UNLV electronic resources are secure according to their risk factors.
- Establish the mandatory use of appropriately secure and strong passwords.
- Establish a standard for creation of strong, but memorable, passwords, the protection of those passwords, and the recommended frequency of change.
- Establish an adjunctive Best Practice on privacy, confidentiality, and security in electronic communications;

In order to manage information security comprehensively, this Best Practice aims to further promote the following goals:

- To ensure that use of IT systems is consistent with sound security principles;
- To ensure that IT systems are used for their intended purposes and meet any compliance requirements;
- To ensure the confidentiality, integrity, availability, and superior performance of IT systems;
- To assure that the core IT network and systems is available to support emergency services in the event of community disaster response needs; and
- To establish standards for addressing security consistency.

**AUDIT CONTROL:** Security audits will inspect the in-use security applications, procedures, and processes of passwords by using this Best Practice, including timeliness of updates, for compliance to security best practice standards. This Best Practice will be audited using the appropriate BS 7799.2:200x Audit Check List, dated 8.08.2005 or later, and through a complete review of all related complaints (security incidents) that occurred after the previous audit.

---

**BEST SECURITY PRACTICE STANDARDS**

---

**INFORMATION SECURITY STANDARDS AND CONTROLS:** UNLV's Best Practice for passwords is a set of general security standards and guidelines that should be applied to each system password creation/selection as appropriate.

***REMEMBER***, if your password is discovered or broken and you determine that someone is using it and accessing your account, please contact the OIT Information Security Office (ISO). The first security measure the ISO will usually recommend will be to change your password. However, the ISO will also want to determine how the account and password were compromised, what the impact of the exposure has had, and whether to investigate, file a complaint with a remote site, or prosecute.

**BSP: 1-1 Password Construction.** All user-level and system-level passwords should conform to the *Password Construction Guidelines* below.

**BSP: 1-2 Password Duration for Users.** All user-level passwords (e.g., email, web, desktop computer, etc.) should be changed at least annually. It is recommended that changes should be made every semester or six months. Passwords that have been or suspected to have been compromised, stolen or guessed should be changed immediately.

**BSP: 1-3 Password Transmission.** Passwords should not be inserted into unencrypted email messages or other forms of electronic communication. Temporary, one-time use, password recovery reset passwords are excepted from this standard.

**BSP: 1-4 Recovery of Forgotten Passwords.** In order to protect confidential information, Help Desk or automated recovery procedures should use non-confidential information for identity verification. If confidential information is the **only** verifiable identity information, the procedure should require only incomplete or partial confidential information over the telephone to be used for verification. Example - It is acceptable to request the last 4 digits or first 3 digits of the SSN but not the full social security number.

**BSP: 1-5 Password Systems.** To maintain accountability for use of computing systems, password systems should be structured so that individual passwords never need to be shared by any other individual. This standards applies to system administrators and site managers.

**BSP: 1-6 Password Don'ts.** In addition to selecting a "good" password, additional rules for keeping your password safe are:

1. Here is a list of "don'ts":
  - Don't reveal a password over the phone to ANYONE
  - Don't reveal a password in an email message
  - Don't reveal a password to ANYONE
  - Don't talk about a password in front of others
  - Don't hint at the format of a password (e.g., "my family name")
  - Don't reveal a password on questionnaires or security forms
  - Don't share a password with family members
  - Don't reveal a password to co-workers while on vacation
  - Don't write down your password in the clear and leave it near your computer or office (Hint: keep it in your wallet if you do write it down!)
  - Don't use the same password for your UNLV-ID that you use as a password for another computer system, as your ATM card PIN number or as your password to a Web site on the Internet.
2. Don't let anyone see you type in your password. Stop typing if you notice someone watching you. Make sure your password is not being echoed whenever you type it in. Some people add extra flourishes of their fingers and hands to mask their movements over the keyboard for any non-casual observers.
3. Make sure you are not on a computer or terminal that is recording your keystrokes as you type in your password. You can usually get rid of such sneaky programs (called keystroke loggers) by rebooting (definitely recommended for Macintoshes) the computer. The safest act to perform upon walking up to a Windows PC in a public cluster is to give it the three-fingered-salute (pressing the 'control', 'alt' and 'delete' keys simultaneously) -- this will reboot it and eliminate most 'Trojan Horse' login programs.
4. Be wary of any program or Web page that asks you for your UNLV-ID and password. Secure UNLV web pages that would ask you for your UNLV-ID account name and password will generally have URLs (Universal Resource Locators) that begin with "https://www.UNLV.edu/" and your browser should

visually indicate that you are typing your UNLV-ID password into a secure page. But if you have never previously seen a particular screen which is prompting you for a UNLV-ID password, it is safest for you to contact OIT help desk and verify the authenticity of the Web page form.

5. Avoid downloading and running programs over the Internet from people or places that you don't know or trust. It is safest to avoid executing any software downloaded from the Internet unless it can be cryptographically verified (via a digital signature or method such as Microsoft's Authenticode(TM) 2.0).
6. Make sure that you are not using insecure protocols (e.g. programs which transmit user account and password information unencrypted) over unsafe networks. This is especially important if you are connecting to UNLV resources with your UNLV-ID from outside the main UNLV network of the residential colleges and computing clusters -- for example, if you are using a computer on a departmental local area network or are connecting to UNLV via the Internet. When in doubt, stop and don't type in your password. If you should use it in an insecure manner or from an insecure location you should change your password as soon as you are back at UNLV or connected safely.
7. Change your password at least as often as required.

## PASSWORD CONSTRUCTION GUIDELINES

### General Construction Guidelines

Passwords are used for various purposes at UNLV. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select usable strong passwords. The first task you perform with your ID at UNLV is also one of the most important to protect it -- choosing a good "**password**". You should make your password memorable but very difficult both for other people to guess and for computer programs to 'brute force attack' it. Best way is by increasing the potential combinations of letters, numbers and other characters used or using a passphrase (which expands the size of the 'search space' for guessers and 'tumbler testers').

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#%&\*( )\_+!~-=\`{ }[]: ";'<>?,./)
- Are minimally 8, preferably 10 or more, alphanumeric characters long.
- Avoids common misspellings and substitutions (e.g., replacing "e" with "3" or "I" with "1")
- Are NOT based on personal information, names of family, etc.
- The password is NOT a word found in a dictionary (English or foreign), or slang, dialect, jargon, etc.
- The password is NOT a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "UNLV", "sanjose", "sanfran", etc. or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Usable passwords have the characteristic that they can be remembered. These are generally passphrases or words that are strung together without separation.

### Password Protection Standards

Do not use the same password for UNLV accounts as for other non-UNLV access (e.g., personal Internet account, etc.). Where possible, don't use the same password for various UNLV access needs. For example, select one password for the department systems and a separate password for database systems.

Do not share UNLV passwords with anyone, except those individuals who are assigned by you to act on your behalf. All passwords are to be treated as sensitive, confidential UNLV information.

If someone demands a password, refer the individual to this document or have them call the Information Security Office.

Do not use the "Remember Password" feature of applications (e.g., Outlook, Firefox, Netscape, etc.).

Do not write passwords down and store them anywhere in your study or work area. Do not store passwords in a non-secure/unencrypted file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least as often as defined above. Passwords may be reused after 10 generations.

If an account or password is suspected to have been compromised, report the incident to the Information Security Office and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the Information Security Office or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

### **Passphrases**

Passphrases are similar but not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks." A passphrase of greater than 10 characters is recommended.

A good passphrase is relatively long, easily remembered and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"Shakespear#Is^Always\*Good\$Reading"

All of the rules that apply to passwords, except the use of words, should be applied to passphrases.

### **Sensible Account And Password Security**

Here are a few good guidelines for creating strong passwords:

1. Use the Construction Guideline.
2. Use at least eight, but preferably 10 or more, characters and symbols.
3. Your password should not be a word found in the dictionary of any known current or dead language -- including Klingon and Elvish!
4. Don't use proper names. This includes all first and last names as well as geographical locations.
5. Don't use numbers based on a particular piece of information that has meaning to you and that can be derived by others (your phone, social security, ID, license plate, VISA credit card number, your birth date, etc).
6. Don't use your initials or those of anyone close to you.
7. Don't attempt to be clever and make your password a derivation (reversed, as-is, shifted by a few characters, a simple substitution code, doubled, etc.) of your ID name or your first or last name.
8. Don't use any information someone could readily obtain about you (your make of car, the street you live on, your residential dorm, etc.).
9. Don't create a password so difficult for you to remember that you will forget it if you don't write it down.

Here are three simple methods for creating "passwords" that are hard to guess or hit upon by accident or force, yet are easy to remember:

1. Use a passphrase as recommended in the Construction Guideline. Create the passphrase using the 3 component model with interspersed special characters.

2. Randomly pick alternating vowels and consonants. Throw in a digit or two (or change a letter or two to a digit) and punctuate. Mix up the case (randomly capitalize for best effect). This will create passwords that have no meaning in the real world but which can still be sounded out (e.g. Me1&BopA).
3. Combine three and four character words with a punctuation character or digit between them. Modify the case of some of the letter and change some of the others to digit or punctuation -- or add digit/punctuation to the beginning or end of the password (e.g. '0Yum|fUn').
4. Try to create passwords that can be easily remembered and pronounceable. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, randomly pick a book, poem or song. Select a phrase from the work and use the first character of each word in the phrase as your password. Capitalize some of the letters and add in at least one punctuation character and digit (or change some of the existing letters to punctuation and/or digit). For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. One recommended method is to use the complete phrase but eliminate or substitute punctuation characters or digits for the spaces - "This%May\*BeOne&Way^To#Remember". NOTE: Do not use these examples as passwords!

### **Recommended Strong "Password" Construction**

***Strong, but memorable "passwords" that resist attacks and guessing, are constructed using a passphrase technique or formula. For general usage it is recommended that general that users construct "PASSPHRASES" that can be remembered with some ease as suggested below. (This recommendation may NOT apply where mandated strong passwords for access to restricted applications and data is required.- check with the system security person)***

**An easy, secure passphrase can be made** using three linked components such as – a building or some personally meaningful number, a unrelated but personal keyword, and a name for the object of the password usage such as "email" or "bank" etc. Put the phrase together using special characters in between each component to create one long passphrase. The whole phrase is really a formula for the passphrase – number, keyword, object (Example: 1234+Hogwarts&email). The 3 components can be put any sequence that is easy for you to remember. Using the above example it could have been "email+Hogwarts&1234" or "Hogwarts&email+1234".