

**1.0 Purpose**

The Password Management Procedures establish the School of Nursing's standards for safeguarding the privacy, confidentiality, and security of electronically stored information, computers, and networks through the use of strong passwords for the Windows Professional operating systems and general password management standards for other operating systems. The use of UCSF computing resources must comply with federal and state laws and regulations and University policy.

This procedure is governed by the HIPAA Security Standard *164.308(a)(5)(ii)(D) Password Management*. Procedures for creating, changing and safeguarding passwords.

**2.0 Definitions**

**2.1 Strong Password:** A strong password is made up of a combination of upper- and lower-case letters and non-alphanumeric characters like the asterisk, exclamation point, dollar sign or percent sign, and involve combining words and characters into a password that can't be found in the dictionary or a hacker's guide.

**3.0 Procedures**

**3.1** Passwords are an important aspect of computer security. A poorly chosen password may result in the compromise of UCSF's entire corporate network. Some of the more common uses include: user-level accounts, web accounts, e-mail 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 strong passwords.

**3.1.1 Require Passwords:** A unique password is required for all accounts including those designated to allow system-level privileges. Examples of system level privileges can include creating and/or deleting a printer queue or creating and/or modifying a user data directory.

**3.1.2 Adhere to Strong Password Security Standards:** Users of the Windows Professional Operating systems must adhere to the following password security standards:

- **Expiration:** Change password every 90 days or less. Passwords will automatically expire every 90 days.
- **Retention:** Once a password is changed, it may not be changed again for eight days.

- **Password History:** Users should not re-use prior passwords. User password history is retained for the last eight passwords to prevent re-use.
- **Password Communication:** Users must keep their passwords secret and not communicate their password to others in any manner. Administrators must not communicate passwords via email or other electronic communication.

**3.1.3 Adhere to General Password Protection Practices:** The following guidelines must be followed when selecting passwords for UCSF computing resources.

- Do not use the same password for UCSF accounts as for other non-UCSF access (e.g., personal ISP account, option trading, benefits, etc.).
- Where possible, don't use the same password for various UCSF access needs. For example, select one password for the Network systems and a separate password for Application systems like Central and GALEN/WebCT.
- 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 anyone, including coworkers, family members or friends in any format, not in conversation, by phone, or in e-mail messages, etc. The only exception is for UCSF School of Nursing IT personnel, who often must use your password to troubleshoot computer problems/issues.
- All passwords are to be treated as sensitive, confidential UCSF School of Nursing information

**3.1.4 Adhere to Administrator Password Standards:** For all system support personnel who are responsible for managing computer and network equipment must adhere to the following standards:

- Where SNMP (Simple Network Management Protocol) is used, the manufacturer's standard default must be changed. This refers to access-level passwords such as "public", "private" and "system".
- Local passwords used to access, setup and configure computer and networking equipment must be different from the

SNMP passwords.

**3.1.5 Password Audits:** Passwords may be randomly audited for compliance using automated software programs or manual methods to decipher or guess user passwords. If a user's password is deciphered or guessed, the user will be required to change it.

**3.1.6 Account Lockouts:** Three invalid attempts to properly enter a user name and password will result in an automatic account lockout. Account lockouts will not be removed or unlocked until the account owner contacts the UCSF School of Nursing IT Customer Support Center (415) 502-8286 and the account owner's identity has been verified.

**3.1.7 Password Changes:** To change a password, a user must first logon to a computer or workstation that is physically attached to the UCSF School of Nursing network. A password cannot be changed from a remote location.

**3.1.8 Adhere to Strong Password Construction Requirements:** Passwords are used for various purposes at UCSF. Some of the more common uses include user level accounts, web accounts, email accounts, voicemail password, etc. Since very few systems have support for one-time tokens (i.e., dynamic passwords that are only used once), everyone should be aware of how to select strong passwords.

Passwords must be a minimum of six (6) characters and contain 3 out of 4 of the following characteristics:

- Upper case characters (A-Z)
- Lower case characters (a-z)
- Digits (0-9)
- Punctuation characters  
(!@#%&\*()\_+|~-=\`{}[]: ";'<>?,./)

**3.1.9 Report Compromised Passwords:** If an account or password has been compromised, change all passwords and report the incident to Information Security by calling the UCSF IT Customer Support Center at (415) 514-4100. If anyone demands your password, refer him or her to this policy and tell him or her to call the UCSF IT Customer Support Center.

## 4.0 Initiation and Control Reporting

## 5.0 Records & Documentation Control

## 6.0 Related Documents

| Document Name   | Procedure No.  |
|---|--|
| University of California Business and Finance Bulletin<br>IS-3<br>Electronic Information Security | <b>IS-3</b><br><a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a> or<br><a href="http://www.ucop.edu/ucophome/policies/bfb/is3.pdf">http://www.ucop.edu/ucophome/policies/bfb/is3.pdf</a> |
| UCSF Information Security and Confidentiality Policy  | <b>650-16</b><br><a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>   |
| Information Security and Confidentiality Policy   | <b>5.01.04</b><br><a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>  |
| Information Access Management Procedures<br>Access Control Procedures                             | <b>60.003</b><br><b>60.011</b><br><a href="http://www.ucsf.edu/hipaa/dept_compliance/">http://www.ucsf.edu/hipaa/dept_compliance/</a>  |

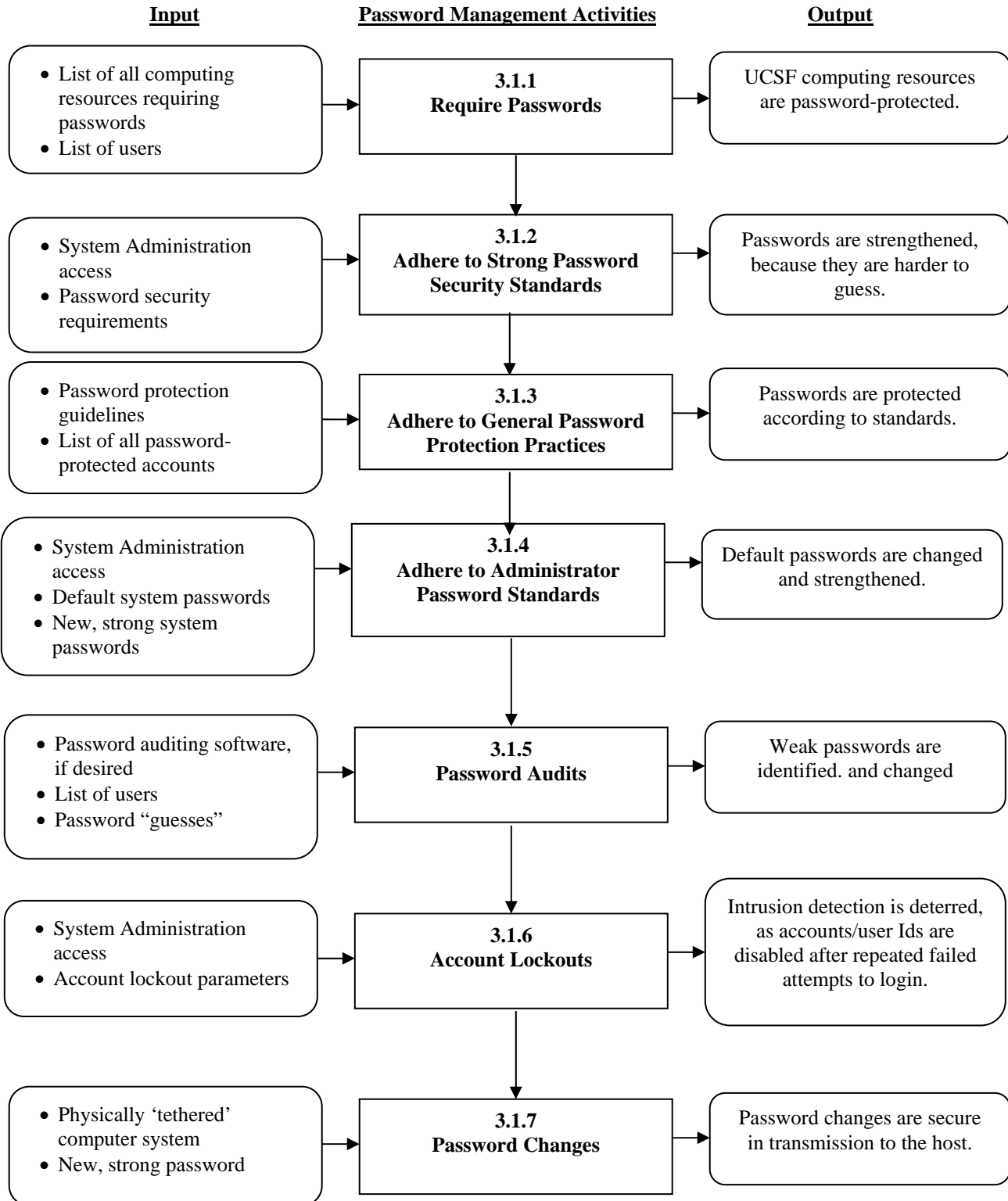
### REVISION RECORD

| Rev. | Date       | Originated by:                     | Description of Change              |
|------|------------|------------------------------------|------------------------------------|
| A    | 02/17/05   | Darlana Torres<br>and Jim Fryhling | Initial Release                    |
| B    | 12/06/2006 | Rob Slaughter                      | Revised for UCSF School of Nursing |

If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.  
 Contains Proprietary Information and is for the use of UCSF only.

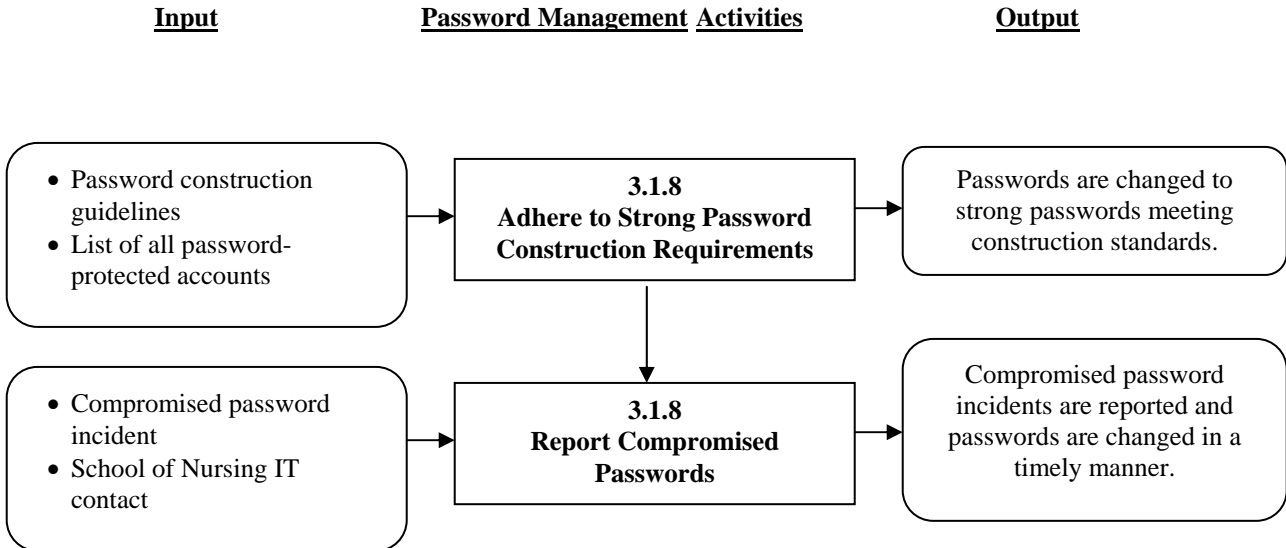
Does not include changes after 12/06/2006

**Appendix A: Password Management Process Flow**



If this is a paper copy, it is **uncontrolled**, and you must verify the on-line revision level before using.  
 Contains Proprietary Information and is for the use of UCSF only.

**Appendix A: Password Management Process Flow, Continued**



If this is a paper copy, it is *uncontrolled*, and you must verify the on-line revision level before using.  
Contains Proprietary Information and is for the use of UCSF only.

Does not include changes after 12/06/2006