

Password Management Procedures

1.0 Purpose

The Password Management Procedures establish the ISU'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 in addition to 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, numbers 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 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.

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 ninety days.
- **Password History:** Users should not re-use prior passwords. User password history is retained for the last eight passwords to prevent re-use.
- **Length:** Password length must be a minimum of six characters.
- **Complexity:** Passwords may not contain your users

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.

Password Management Procedures

name or any part of your full name.

- **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.
- Select a separate password to be used for an NT account and a UNIX account.
- 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.
- All passwords are to be treated as sensitive, confidential UCSF information

3.1.4 Adhere to Administrator Password Standards: 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.

Password Management Procedures

3.1.5 Account Lockouts: Five invalid attempts to properly enter a user name and password will result in an automatic account lockout. Account will automatically unlock after 30 minutes.

3.1.6 Adhere to Strong Password Construction Requirements:

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
(!@#\$%^&*()_+|~-=\`{ }[]: ";'<>?,./)

3.1.7 Report Compromised Passwords: If an account or password has been compromised, change all passwords and report the incident to Information Security by calling the IT Customer Support Center at (415) 514-4100.

4.0 Initiation and Control Reporting

5.0 Records & Documentation Control

6.0 Related Documents

Document Name	Procedure No.
---------------	---------------

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.

Password Management Procedures

University of California Business and Finance Bulletin IS-3 Electronic Information Security	IS-3 http://www.ucsf.edu/hipaa/dept_compliance/ or http://www.ucop.edu/ucophome/policies/bfb/is3.pdf
UCSF Information Security and Confidentiality Policy	650-16 http://www.ucsf.edu/hipaa/dept_compliance/
Information Security and Confidentiality Policy	5.01.04 http://www.ucsf.edu/hipaa/dept_compliance/
Information Access Management Procedures Access Control Procedures	60.003 60.011 http://www.ucsf.edu/hipaa/dept_compliance/

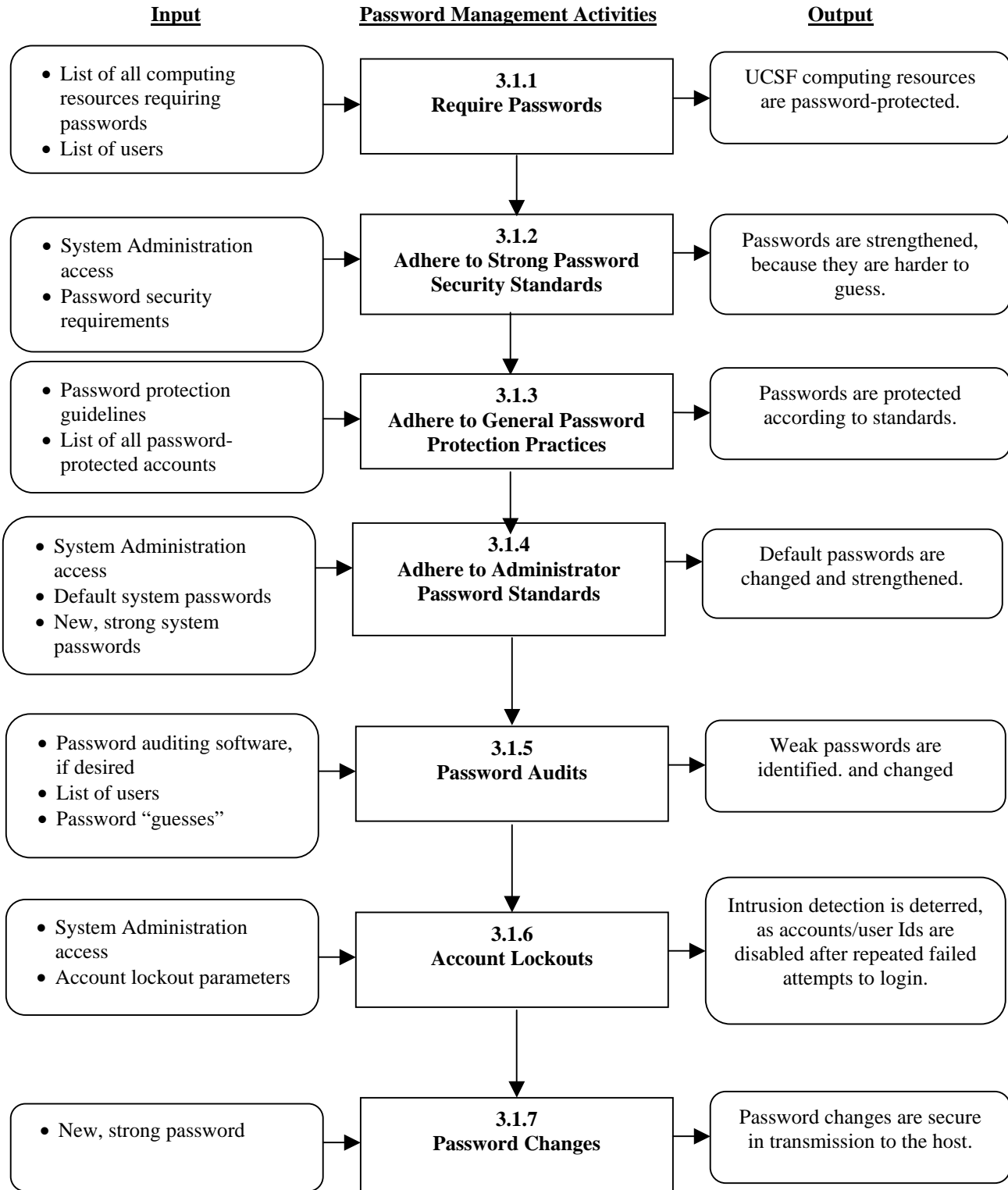
REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	02/17/05	Darlana Torres and Jim Fryhling	Initial Release
B		Todd Lawrence	Converted to S/Med Template

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.

Password Management Procedures

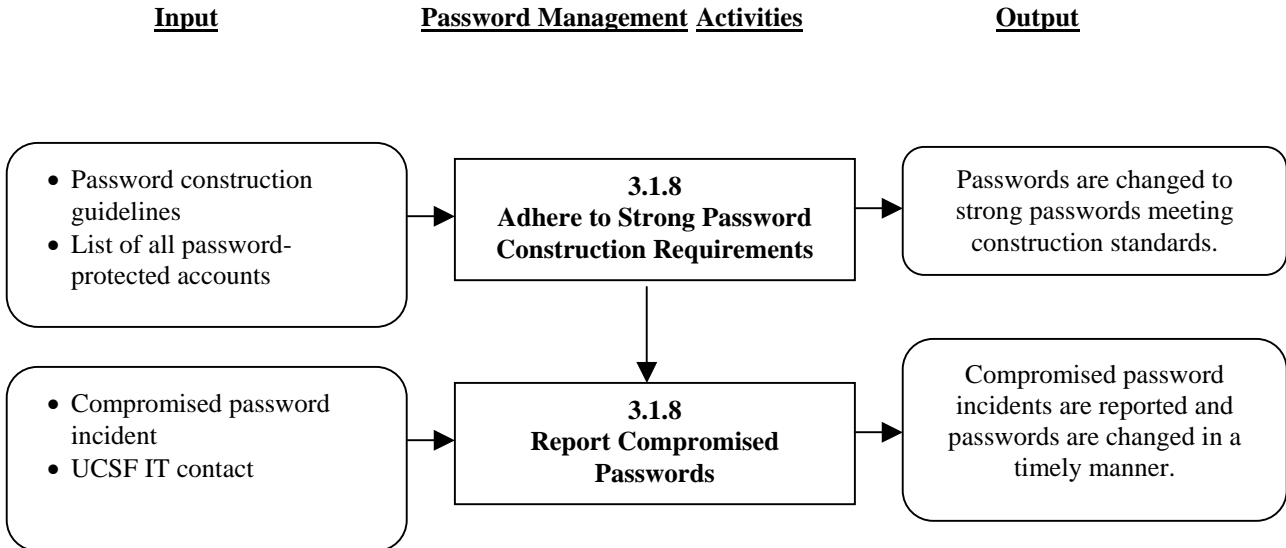
Appendix A: Password Management Process Flow



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.

Password Management Procedures

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.