

1.0 Purpose

The purpose of these procedures is to define standards for controlling and validating access to facilities in which electronic information systems are housed. This document addresses the following topics:

- The Facility Security Plan (section 3.1)
- Facility Access Control and Validation (section 3.2)
- Facilities Maintenance Records (section 3.3)
- Contingency Operations Plan (section 3.4)

2.0 Definitions

2.1 Access Control: The process of user authentication, granting, and limiting access to facility, application and system resources to only authorized individuals, programs, processes, or systems.

2.2 Workforce: All faculty, staff, students, trainees, volunteers, and business associates who access restricted or confidential information during the course of their duties.

3.0 Procedures

3.1 Facility Security Plan Procedures: As UCSF is an open to the public institution you cannot rely solely on the existing perimeter access control plan to protect sensitive areas. You must implement procedures to limit physical access to electronic information systems and the facility or facilities (suite, office or department) in which they are housed, while ensuring that properly authorized access is allowed. *Note:* This procedure supports the Information Access Management Procedures # 60.002 and the System Access Control Procedures # 60.011.

3.1.1 Define locations requiring facility access controls: You (Managers and or CSCs) must identify the areas under your control that contain systems as well as locations that allow connectivity to: system elements, supporting services such as electric power, backup media, and any other elements required for system operation.

3.1.2 Define facility access controls: Define facility access controls to safeguard both the facility and the equipment housed within the facility from unauthorized access, tampering or theft. Part of your plan can include that UCSF and the UCSF Medical Center have a closed perimeter after hours.

3.1.3 Define implementation of access controls: Managers/CSCs will need to define the specific methods used to limit access to their suites, offices or department areas as identified by 3.1.1 above. All systems, whether they are mechanical or electronic, must comply with UCSF and/or

UCSF Medical Center systems.

3.1.4 Define access control validation: Managers /CSCs are responsible for setting up a process to review and validate the effectiveness of their selected facility access controls in each area during normal business hours and at other times – particularly when the areas would typically be unoccupied. This review and validation should be done quarterly.

3.2 Facility Access Control and Validation Procedures:

Managers/CSCs are responsible for implementing procedures to control and validate an individual's physical access to facilities and systems that contain restricted or confidential information. Managers should review this process quarterly.

3.2.1 Restrict and control access to facilities and systems:

Access to facilities and systems that contain restricted or confidential information must be restricted to *authorized* workforce members according to the individual's job assignment or job function. Managers should ensure that any incidents of unauthorized entry or access are reported immediately.

3.2.2 Use authentication procedures:

Prior to granting access to facilities and systems that contain restricted or confidential information, utilize established authentication methods such as checking ID, or requiring access card or a sign in.

3.2.3 Supervise workforce:

Supervise all workforce members who have been granted physical access while they are present in the facilities and working on systems that contain restricted or confidential information.

3.2.4 Maintain access logs:

Maintain a log listing individual names, date and entry and departure times.

3.2.5 Require visible identification:

All UCSF employees must have a photo ID as stated in UCSF Policy 150-17 <http://policies.ucsf.edu/150/15017.htm>. Departments that wish to establish "restricted areas" are encouraged to require the visible wearing of UCSF identification for individuals prior to granting access to facilities or systems that contain restricted or confidential information. Unescorted visitors and those who do not have visible identification will not to be granted access without first

undergoing established authentication and clearance procedures. Workforce members are advised to challenge unescorted visitors and those who are not wearing visible identification and report these incidents to management.

3.2.6 Maintain authentication procedures

At least annually managers must review and update authentication procedures as well as access rights to facilities and systems that contain restricted or confidential information.

3.3 Facilities Maintenance Records Procedures: Implement the following procedures when documenting repairs and modifications to physical components of facilities related to security from which one can gain access to restricted or confidential information. Either the Lock Shop or Engineering will maintain these records.

3.3.1 Define security controls when transporting offsite:

Employ appropriate security controls when sending the physical components of facilities off premises for repairs or modification.

3.3.2 Verify authorization of repair personnel: Verify that personnel who perform repairs and services have been previously authorized.

3.3.3 Log details of repairs and modifications: Maintain documented records of repairs and modifications and include the following:

- Date and time repairs and/or modifications are performed
- Name and signature of person performing repair or modification
- Suspected or actual faults
- Repairs and/or modifications made

3.4 Contingency Operations Plan: System managers, system owners, and department managers must implement procedures for developing a plan to allow physical access to facilities in which restricted or confidential information is housed in the event of an emergency. Who can and cannot carry material in and out your site? Who besides UCSF Emergency Responders (Police/ Security, EH&S, Engineers, etc.) is authorized to access your site in the event of an emergency?

3.4.1 Identify facilities: Identify the facilities that will need to be accessed in the event of an emergency.

3.4.2 Identify facility access control contacts: Identify the individuals and prepare a contact list including name, phone number, email address for those who are responsible for controlling access to the facilities that will need to be accessed in the event of an emergency. Distribute the list specified in the Emergency Mode Operation Plan and the Disaster Recover Plan. For further details, refer to the Contingency Plan Procedures 60.006.

3.4.3 Define communication method for facility access control contacts: Define methods of communicating with facility access control contacts before, during and after an emergency.

3.4.4 Define facility access control and validation requirements: Define the appropriate authentication procedures for the facility to ensure that only authorized access is granted to the facility in the event of an emergency.

4.0 Initiation and Control Reporting

5.0 Records & Documentation Control

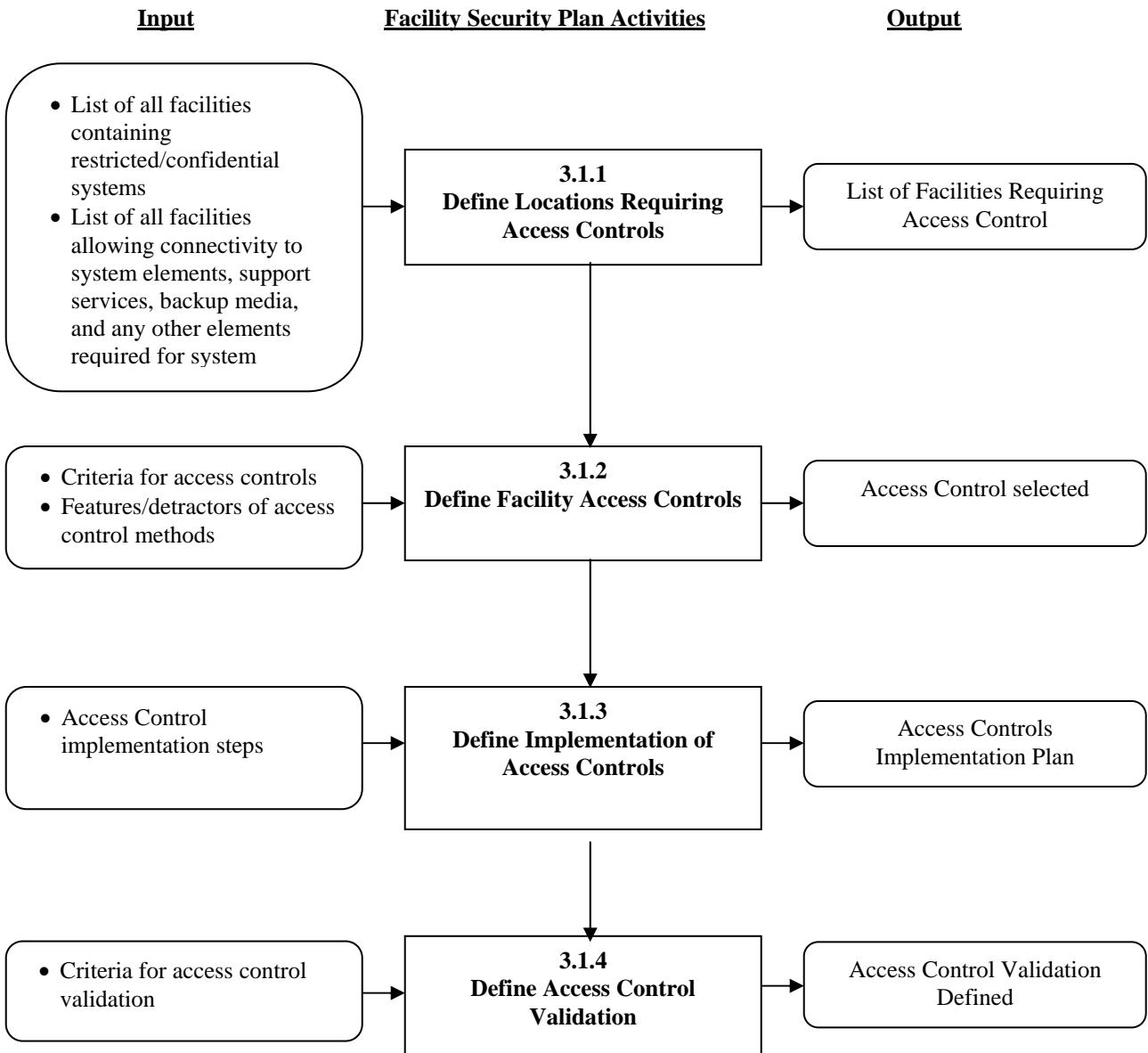
6.0 Related Documents

Document Name	Procedure No.
HIPAA Security Rules: Facility Access Controls Information Access Management Access Control	164.310(a)(1) 164.308(a)(4) 164.312(a)(1) http://www.ucsf.edu/hipaa/d/ept_compliance/
Special Publication: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule - National Institute of Standards and Technology (NIST)	SP 800-66 http://www.ucsf.edu/hipaa/d/ept_compliance/
University of California Business and Finance Bulletin IS-3 Electronic Information Security	IS-3 http://www.ucsf.edu/hipaa/d/ept_compliance/ or http://www.ucop.edu/ucophone/policies/bfb/is3.pdf
Identification Cards Policy (UCSF)	150-17 http://policies.ucsf.edu/150/15017.htm .
Information Security and Confidentiality Policy (UCSF Medical Center)	5.01.04 http://www.ucsf.edu/hipaa/d/ept_compliance/
Information Security and Confidentiality Policy (UCSF)	650-16 http://www.ucsf.edu/hipaa/d/ept_compliance/
Information Access Management Procedures Contingency Plan Procedures System Access Controls Procedures	60.003 60.006 60.011 http://www.ucsf.edu/hipaa/d/ept_compliance/

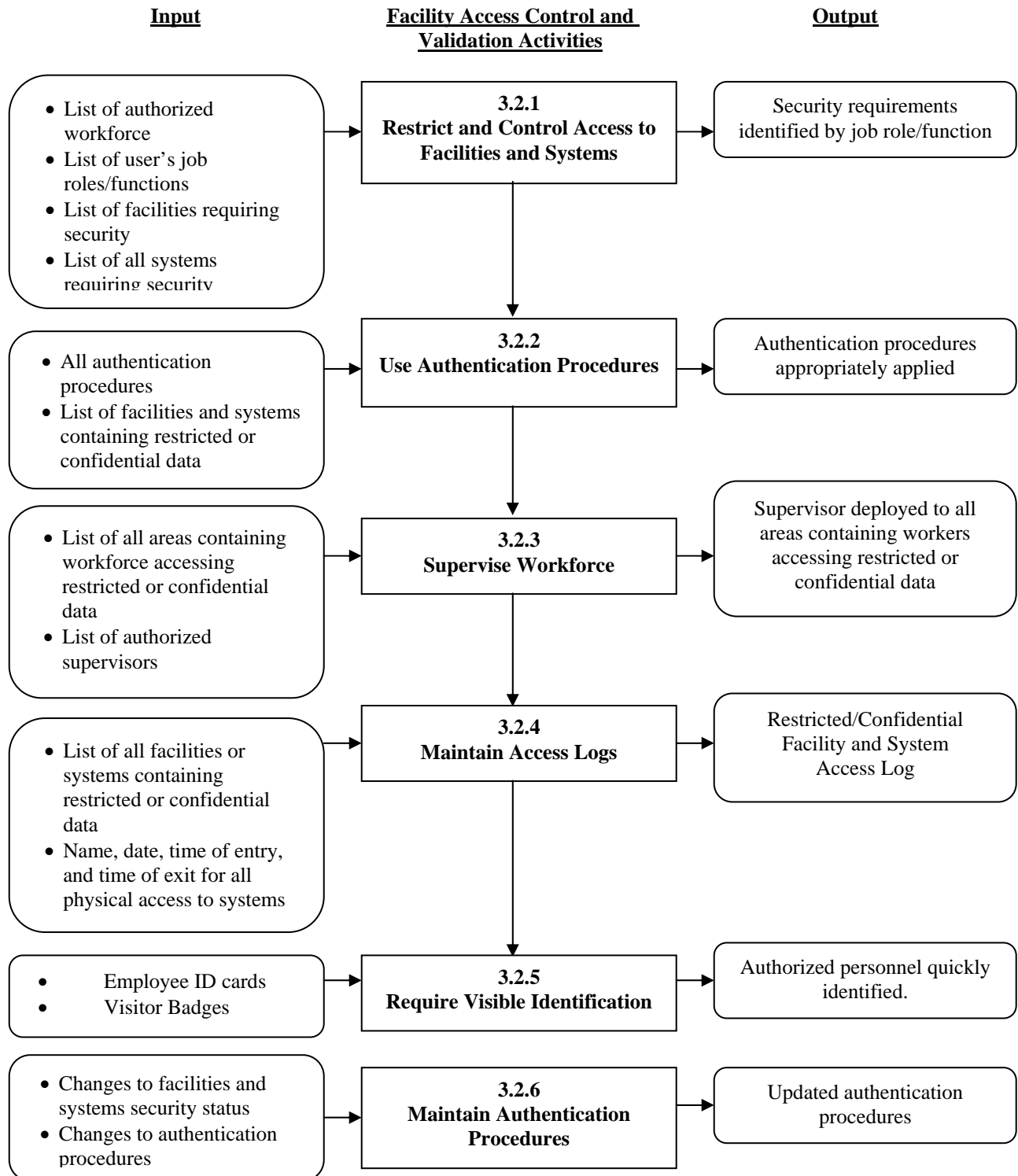
REVISION RECORD

Rev.	Date	Originated by:	Description of Change
A	02/07/2005	Peter Balestreri, Mike Sorensen, Ben Gordon, and Robert Hunn	Initial Release
B	11/27/2006	Rob Slaughter	Revised for School of Nursing

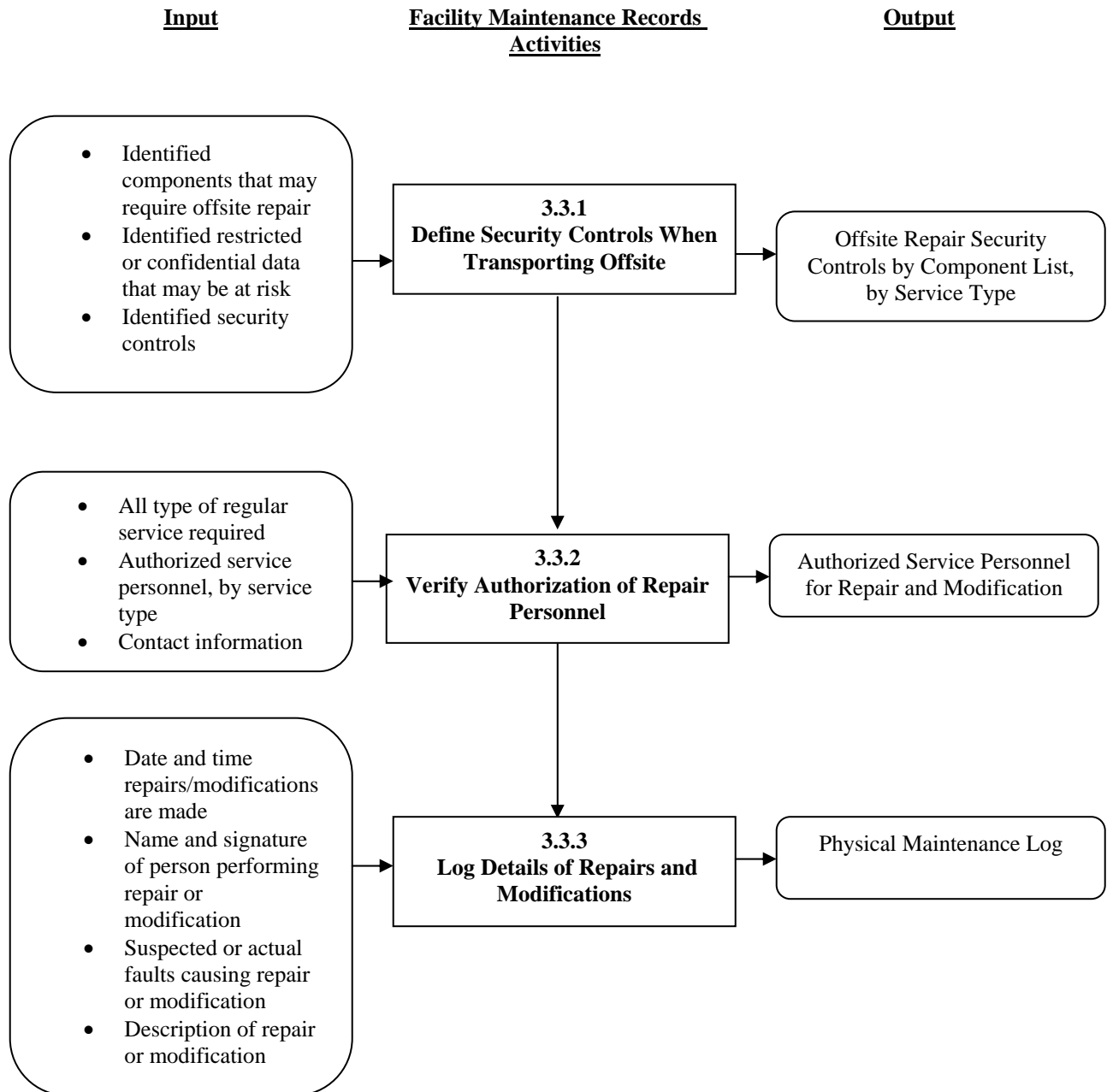
Appendix A: Facility Security Plan Process Flow



Appendix B: Facility Access Control and Validation Process Flow



Appendix C: Facility Maintenance Records Process Flow



Appendix D: Contingency Operations Plan Process Flow

