Compliance Procedure

Title: **Safeguard IT Systems and Data Not Residing in Primary Facility**
Reference Number: **7.2.3**

Purpose

The purpose of this procedure is to define the process whereby IT Systems and Data not residing in the primary data center facility shall be protected from improper or unauthorized access. This includes physical security and logical security methods.

Procedures & Related Information

OCCS takes particular precautions to ensure that remote facilities such as computer labs, technology wire closets, equipment storage locations, off site media storage locations and disaster recovery locations are kept secure and fitted with access controls.

All OCCS remote facilities are placed on the Best Access card access system which has it's monitoring hub (surveillance & management) in the primary computer operations console area within E&CS.

Such facilities controlled by Best Access equipment have their doors equipment with a proximity card reader, requiring anyone who wants access to have an appropriately predefined identification card. Privileges and access authority is requested and granted on an as needed basis by management staff and id cards are populated in the Campus Card Center (not run by OCCS staff).

All OCCS facilities have locks on their doors. Most are proximity card locks however some have only standard keyed door locks. New building projects and renovations are moved to the magnetic stripe proximity lock system.

OCCS remote facilities are equipment with adequate power and air conditioning. Glass in doors and windows have been eliminated as part of these facilities whenever possible.

Physical keys are kept to a minimum and distributed to staff only on an as needed basis. Magnetic card swipe IDs are issued to specific staff with specific access abilities.

Computer Operations maintains a key for many functional areas of the campus, checking out these keys to appropriate vendors and staff while logging the usage of such keys. Keys are inventoried and logged at the beginning of each shift to ensure these keys are returned in a timely manner. Such records show the name & company of the party requesting the key, the time that they take the key and the time that the key is returned. Identification of those requesting the keys is required.

Such logs are maintained for historical purposes for 60 days should an issue require revisiting the detail.

Computer Operations also monitors the Best Access video surveillance console where all entries are logged, while particular locations are subject to video monitoring.

Last Review Date: **February 27, 2007**