Compliance Procedure

Title: **Controlled Access to Hardware and Network Facilities**
Reference Number: **7.2.6**

Purpose

The purpose of this procedure is to define the process by which OCCS shall control access to facilities where hardware and network related equipment, wiring, and displays are housed. OCCS expects all staff members to be cognizant of the financial investment that the University has made in computing equipment and facilities. OCCS considers any facility that houses technology equipment, remote or onsite, to be a controlled access environment. Special attention must be given to non-OCCS staff person being allowed to enter and remain in that facility. Additionally, not all OCCS staff have equal rights and access privileges with regard to space and entry to OCCS facilities.

Procedures & Related Information

All staff members have electronic access card entry keys to allow them to enter those areas where they have a legitimate business need, including the Open Office Area and Administration Area. Select employees, based on business need; also have access to the server room. Primarily, the Computer Operations staff and Network Support staff have a legitimate need to be in the server room. Most other business can be accomplished without physical entry into the room. Server room access is granted to only key individuals and management.

The computer room staff is to remain present in the Console Command/Print Area at all times. Facilities are not to be left un-staffed.

OCCS has purchased and installed a card key entry system with an associated computer server, named BullDog, which resides in the server room cabinet D7. This cabinet has a combination lock in which only OCCS Security staff have access. This server controls the automatic opening and automatic locking of key doors to the E&CS facility, OCCS Labs, and OCCS wire closets. During normal work hours, all non-employees wishing to enter the facilities must be routed through the front office staff for the issuance of temporary badges and check-in processing. Staff will be called and alerted of visitors by the front office staff or service desk personnel.

OCCS staff members are asked to carry their electronic card keys at all times. Staff members are not to leave server room or open office area doors propped open or cracked. All doors entering OCCS have alarm monitoring tools associated with them (audible or video). Console Command area staff monitors them using video surveillance.

Vendors who might require admittance to the server room for repair of computing equipment or environmental equipment will be assigned an OCCS Comm Guest access card. This card will allow access to server room and communications closets from M-F (8 am – 5 pm). Escorting vendors by Operations staff may be required. No equipment or software is to be taken out of service, modified, or moved without full knowledge and approval of management. Overall concern is to be given to the continuance of critical services – not unplanned visits by vendor representatives. Vendor presence in the facility is to be logged in the operator logbook – both starting and stop times.

Any issues relating to attempts to gain access by unauthorized persons should be quickly relayed to campus security @ 3-4000 and to OCCS management. Supervision should be alerted for any problem resolution purposes required. All issues and follow-up information should be documented in the operations logbook, including phone calls received and made during an incident.

Facility tours and demonstrations requiring entry into the server room should include a discussion with all potential visitors regarding the critical nature of our business and the need to not touch anything, push anything, nor lean on anything nor take anything.   Clearly, critical and timely service functions are constantly going on in that environment.   Working around non-staff people and those related disruptions should be kept to a minimum.

Remote facilities to include computer labs and technology closets within multiple buildings are also under the card access system operated by OCCS.   Those staff members who have specific needs to access that space shall be given appropriate access to visit and utilize those spaces in an unobstructed manner.

Operations staff members shall exercise great care to ensure that remote door entry capabilities when asked via the telephone to open a specific door.

Last Review Date: February 27, 2007