Access to Communications Closets
08/01/2013

This document presents options for access to Communication Closets. Access to these closets must be controlled for several reasons:

• Communications closets are part of resources critical to the day-to-day operation of CSU. Any inappropriate activities in these closets may result in loss of critical services, including Emergency 911 service.

• Access to these closets presents the opportunity to conduct illegal activities, such as tapping into phone calls and/or data transmissions.

• The communication networks are built to the precise and stringent standards of CommScope Systimax. Post construction, all communication networks are certified by CommScope Systimax, and guaranteed to perform at rated capacity for 20 years. CSU’s Department of Telecommunications and ACNS (hereafter referred to as “ACNS”) personnel are certified to perform work according to maintain this certification. Therefore, ACNS personnel are allowed to work on the network components without jeopardizing the warranty. Unauthorized personnel working on the network components without the proper understanding of the CommScope Systimax standards and University standards are jeopardizing the warranty and substantial financial investment.

• ACNS is responsible for the physical telephone and data infrastructure at the University. ACNS invests in all infrastructure projects on campus and performs the design, bid, contractor oversight, post-installation certification, and maintenance of the installed infrastructure. In addition, ACNS assumes the responsibility for the physical infrastructure for voice and data, to ensure it meets industry and University standards.

There are valid reasons for users to access the communication closets. Therefore, ACNS has the following policy regarding access:

1. Upon this written request, ACNS will issue only one communications closet key to a Subnet Manager. At the sole discretion of the Subnet Manager, this key may be shared with a second individual designated by the Subnet Manager. These two individuals must pass background checks, conducted by an external entity approved to do so by the University. Background checks will be coordinated by CSU Telecommunications. The cost of these background checks will be borne by the Department/Unit. Only these two individuals shall enter the communication closet(s) accessed by this key. Additional keys shall not be provided or acquired by any other means.

2. Both individuals must be regular, full-time CSU employees.

3. In case of a lost, stolen or otherwise misplaced key, the communications closet(s) shall be re-keyed at the expense of the Department, College or Unit.

4. The Subnet Manager or designee must not conduct any activity that might affect the telephone, fiber or any other service facilitated by components or infrastructure located in the closet(s). The closet(s) wiring and patch panel(s) shall not be accessed or modified in any way. The Subnet Manager or designee agrees not to mount or install equipment in the closet(s) without first obtaining written approval from the ACNS. All data equipment installed in the closet shall be rack mounted, and subject to the pre-approval of ACNS.
5. The Subnet Manager and Departmental, College or Unit Director may choose one of the options below for the data network:

**Option A: ACNS shall be completely responsible for the data/voice network.**

- The Subnet Manager and Departmental, College or Unit Director agrees not to access or modify the physical data/voice network in any way.
- ACNS agrees to issue a key to the Subnet Manager and Departmental, College or Unit Director, and requests that the Subnet Manager participate in operational activities only, e.g., rebooting network devices and Uninterrupted Power Supplies (UPS), in coordination with ACNS. The Subnet Manager is requested to supply contact information on Schedule A, attached to this request.
- ACNS will activate existing data jacks (e.g. in an office or computer lab), assuming unused switch ports are available, without a labor charge to the Department or College. ACNS shall charge a standard rate for CommScope Systimax patch cord(s) required to activate both ends of a data connection. When new data jack(s) are required, ACNS shall charge for materials and labor at rates.

**Option B: The Subnet Manager and Departmental, College or Unit Director are permitted to add, move and change data patch cords only.** Subnet Manager and Departmental, College or Unit Director agree to be responsible for modification of the data network in accord with CommScope Systimax and University specifications. Subnet managers agree to and understand that:

- Modifications of the data network may involve inadvertent interference with the VOIP network along with 911 location information, and authorized personnel making these changes assume all responsibility and liability for such actions.
- Only CommScope Systimax patch cords of the appropriate length may be used to patch connections. The Subnet Manager must be particularly careful to eliminate stress or severe bends on the patch cords and to “dress” the cords appropriately along the cable guides.
- Under no circumstance shall patch cords of any color than white be used for VOIP cabling, inter-switch cabling, or inter-IDF cabling without prior arrangements with ACNS/Telecommunications.
- The following patch cord color scheme must be adhered to:
  - Red/Grey: Data
  - White: VOIP
  - Green: Security Cameras, CardKey, Meters, EMS, Facilities
  - Violet: A/V Data
  - Orange: Switch-switch links
  - Light blue: Departmental specific
  - Yellow: Wireless
- Under no circumstances shall the back-end of the network (i.e. the network from the patch panel to the wall jack) be touched. The data network must remain within CommScope Systimax and University specifications.
6. Additional communication closet and Voice over IP (VOIP) standards that apply to both options A and B.
   - Communication closets are not to be used for storage, even on a temporary basis.
   - ACNS requests to be advised of any maintenance issues concerning the closet (broken locks, leaky pipes, etc.).
   - Communication closet doors cannot be left unlocked, propped open or left unattended without being locked.
   - Any non ACNS equipment in closets must be approved in advance, in writing or e-mail by ACNS staff.
   - Any pre-approved, departmental equipment mounted in closets must be labeled as to the machine name and contact information.
   - ACNS will have sole administrative access to all components in voice path.
   - Adds/changes/deletes of VOIP sets to be processed through ACNS.
   - Physical install and verification of VOIP sets to be done by ACNS.

7. The Subnet Manager and Departmental, College or Unit Director shall be responsible for the enforcement of this agreement. Failure to abide by this agreement may result in loss of access to communications closets.

8. ACNS shall annually review with the subnet manager and/or their designee compliance with this agreement, at which time standards, closets and procedures will be inspected and discussed. Failure to adhere to the terms of this agreement will result in revocation of key(s).
We, the undersigned, have read, understand and agree to all the provisions herein stated in this document.

Option selected 5.A _____ 5.B _____

Subnet Manager:

Signed ________________________________ Date ___________________

Printed Name _________________________ EID ___________________

Key ID ________________ Key Location

Background check completed on (date):

Subnet Manager's Designee:

Signed ________________________________ Date ___________________

Printed Name _________________________ EID ___________________

Key ID ________________ Key Location

Background check completed on (date):

College/Department/Unit Director:

Signed ________________________________ Date ___________________

Printed Name _________________________

ACNS Director:

Signed ________________________________ Date ___________________

Printed Name: Scott K. Baily
Schedule A
Data Network Contact Information

The following information is provided in support of the joint data networking activities conducted under the centralized/decentralized model for networking at the University.

1. Primary contact:

Name: ___________________________ Office phone number: ___________________________
Cell Number: ______________________ Home phone number: ___________________________
E-mail address: ____________________
Period for primary contact, days and hours (e.g. 7 AM - 5 PM M-F): _______________________
Instructions for contact during off-hours: ________________________________

2. Secondary contact:

Name: ___________________________ Office phone number: ___________________________
Cell Number: ______________________ Home phone number: ___________________________
E-mail address: ____________________
Period for primary contact, days and hours (e.g. 7 AM - 5 PM M-F): _______________________
Instructions for contact during off-hours: ________________________________

3. Other instructions: