# Communication Room Access Agreement
Version 4.2, revision 03/17/2023

## Rationale:
- **Life-safety, business continuity resource**: Communications rooms are part of resources critical to the day-to-day operation of CSU. Any inappropriate activities in these rooms may result in loss of critical services, including Emergency 911 service.
- **Protection of data**: Access to these rooms presents the opportunity to conduct illegal activities, such as tapping into phone calls and/or data transmissions.
- **Building warranty:**The communication networks are built to the stringent standards of CommScope Systimax.  Post construction, all communication networks are certified and guaranteed to perform at rated capacity for 20 years. CSU's Networking and Telecommunications Services personnel are certified to perform work to maintain this certification. Unauthorized personnel  working on the network components jeopardize the warranty and substantial financial  investment.
- **Responsible party**: Networking and Telecommunications is responsible for, and access to, the telephone and data  infrastructure at the University. Networking and Telecommunications invests in infrastructure projects on campus and   performs the design, bid, contractor oversight, post-installation certification, and maintenance   of the installed infrastructure. Networking and Telecommunications assumes the responsibility for the physical  infrastructure for voice and data to ensure it meets industry and University standards.

## Access:
NOTE: As of July 1, 2018, newly constructed communication rooms are cardkey access only.
- Physical keys:
  - Networking and Telecommunications will issue only one physical communications room key to a College/Dept  primary IT Manager. This key may be shared with a secondary designated by the IT  Manager and listed on this form.
  - Only these two individuals shall enter the communication room(s) accessed by this physical key.
  - Additional keys shall not be provided or acquired by any other means.
  - The key must always remain secured if it is not in the IT Manager's possession.
  - In case of lost, stolen or otherwise misplaced key, the communications room(s) shall be  re-keyed at the expense of the Department, College or Unit.
- Cardkey:
  - Cardkey access may be granted to IT staff directly reporting and having direct business needs for accessing the communication rooms.   The primary IT manager can request such access by co-signing this form and being responsible for actions of their IT staff member.
- All individuals requesting access must pass background checks.  The cost of these background checks will be borne by the Department/Unit if one has not yet been performed on the CSU staff member.
- All individuals requesting access must be regular, full-time CSU employees.
- The IT 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 room(s).

- The room(s') wiring and patch panel(s) shall not be modified in any way.
- No equipment can be installed in the room(s) without first obtaining written approval from Networking and Telecommunications ([https://telecom.colostate.edu/wp-content/uploads/sites/19/2017/09/Communications-Room-Equipment-Installation-August-2017.pdf](https://telecom.colostate.edu/wp-content/uploads/sites/19/2017/09/Communications-Room-Equipment-Installation-August-2017.pdf))

## Procedures:

- Equipment cannot be rebooted, unplugged, moved or otherwise potentially cause service interruption without Networking and Telecommunications staff's immediate direction.
- No storage of any type is permitted in communication rooms.
- Doors are not to be propped open. Last person leaving the room is responsible for any subsequent damage or service interruptions due to improperly securing of the room or unauthorized access.
- Only red, gray, white or departmental specific light-blue cables may be added/moved/removed. Under no circumstance are any other cabling, infrastructure or equipment to be modified. Any tampering with other colored cables will result in that individual accepting liability for business continuity or life-safety connections in that communication room.
- Cables will be of proper length, color, type and routing. Cables are not to have excessive loop nor be strung too tightly. Cables are to exit the switch port, immediately be routed through cable management to the patch panel. The patch cord color scheme must be adhered to:

  Red/Grey: Data
  White: VOIP/Data
  Green: Facilities
  Violet: Audio/Visual
  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.

## Charges:

- Networking and Telecommunications will install data cables in network rooms free of charge when a service order is placed (http://telecomserviceorder.colostate.edu).
- Moving of non-red, non-gray or non-light-blue cabling will result in service charges.
- Redoing cabling not patched per above procedures will result in service charges.
- Removal of trash or stored equipment will result in service charges.

## Enforcement:

- The IT 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 communication rooms or result in service charges.
- Networking and Telecommunications shall annually review with the IT Manager compliance with this agreement, at which time standards, rooms and procedures will be inspected and discussed.

## **Signatures**:

We, the undersigned, have read, understand and agree to all the provisions herein stated in this document.

**Primary IT Manager**

Signature_____Date _____

Printed Name _____

eID _____

Desk phone#_____Cellphone #_____

Bldg# you need a key for_____

Room#(s) you need a key for_____


**Secondary IT Manager (physical key) or IT staff designated by IT manager (cardkey)**

Signature_____Date _____

Printed Name _____

eID _____

Desk phone#_____Cellphone #_____


**College/Department/Unit Director:**

Signature_____Date _____

Printed Name _____

eID _____


**Manager of Networking and Telecommunications:**

Signature_____Date _____