Description and Mission

The College of Communication Technology Services Desk provides technology infrastructure, maintenance, first responder support and escalated IT solutions for departments and units within the College.

Technology Services supports students, faculty and staff of the College of Communication. Support is provided for, but is not limited to, the major departments of the College which include the Dean's Office, Advertising, Communication Sciences and Disorders, Communication Studies, Journalism, KUT Radio, Radio-Television-Film and Texas Student Media. Various academic and research units within the College are also supported.

Supported Buildings

Technology Services supports IT in the buildings that the College occupies. These buildings include:

- **BMC** the Belo Center for New Media
- **CMA** the Jesse H. Jones. Communication Center Building A
- **CMB** the Jesse H. Jones. Communication Center Building B
- **HSM** the William Randolph Hearst Building

Hours of Operation, Location and Contact Info:

The Technology Services Desks are located in CMA 3.104 and BMC 5.104

Regular hours of operation are Monday through Friday, 8am to 5pm.

Limited support for classrooms and departments is provided from 7am to 7:45am and 5pm to 8pm.

The Technology Services Desk can be contacted via phone at 512-471-1199. The phone is answered by staff between the hours of 7am-8pm, M-F. From 5pm-8pm M-F, the phone is answered as the reduced staffing allows.

Technology Services tracks IT tickets through WebHelpDesk. Patrons can submit trouble tickets directly to WebHelpDesk, by calling the Service Desk phone at 471-1199, emailing comm-help@austin.utexas.edu, or by walk-in to our CMA and BMC offices.

Support is not available during university holidays and building maintenance closures. Evening support may be reduced during intersessions.

Services Provided

Technology Services provides the following services:

- Desktop computer support to College of Communication Students, Faculty, and Staff for College of Communication owned computers
- Computer imaging and deployment
- College Classroom AV support
- College computer lab support
- Wired Ethernet connectivity
- Computer relocation
- Purchasing recommendation and consultation
- Network shares for classes, staff, faculty and approved special projects.
- Monitoring for software licensing and information security compliance

First responder priority is given to classrooms and computer labs. Business systems, research units and others are given second priority during times of heavy demand.

Second tier support that requires more in-depth troubleshooting will be handled internally within Technology Services or transferred where appropriate to departmental tech units KUT or ITS.

The Technology Services group maintains a standardized desktop computing environment through purchasing standards, inventory life cycles, and management tools. A consistent level of service with desktop management is provided using tools such as

- Active Directory for EID login and account management,
- Group Policy for common Windows settings,
- Apple Remote Desktop for Mac management and remote control,
- LANDesk for patch management, inventory, remote control, package deployment and scripting,
- Deploy Studio for Mac OS deployment.

More information on services can be found at [http://moody.utexas.edu/technology](http://moody.utexas.edu/technology)

Knowledgebase articles, policies, and procedures can be found here at [https://wikis.utexas.edu/display/comm/Technology+Knowledgebase](https://wikis.utexas.edu/display/comm/Technology+Knowledgebase)
Patron Responsibilities

Technology Services patrons agree to adhere to the university's Acceptable Use Policy and will manage data in a responsible manner. In addition, patrons of College of Communication technology resources will abide by university encryption policies for laptop devices.

Patrons agree that Technology Services administrative accounts will be maintained on all supported systems and that access to those systems. Technology Services will not access offices, work systems or network shares unless required for troubleshooting a specific problem or security risk.