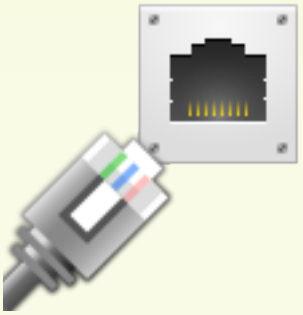
08:18:05 NETWORK ACCESS

1. The network, both wired and wireless, is ChSCC's first line of defense against viruses, worms, hackers, and individual misuse that can compromise critical computer systems and data that support ChSCC's business.

2. This policy applies to all ChSCC personnel including staff/faculty, adjuncts, full-time and part-time, and students.



3. ChSCC Technology has the responsibility and authority to scan computers attached to the ChSCC networks to ensure appropriate security and support network operations and performance.

4. Technology reserves the right to restrict access to services and resources that are disruptive to the network or pose a threat to the college information security, audit or accreditation status.

5. No change to any wired/wireless network device, hub, switch, ports or other network device will be done without prior Technology Network Services approval.

6. Wireless access points should be installed in physically secure areas accessible only by authorized Technology personnel to prevent unauthorized access and physical tampering.

7. Wireless clients accessing the campus wired infrastructure must meet certain data networking and security standards to ensure only authorized and authenticated users are able to connect.

8. Requests for any Network support must be made through the Technology Work Order system prior to the work being done. Emergency situations will be handled on a case by case basis.

For further guidance, read ChSCC 08:18:05 Network Access:

technology.chattanoogastate.edu/policies-procedures

Chattanooga State
Community College