

Colorado School of Mines

Campus Wireless Network Infrastructure Policy

Executive Summary

This policy assigns responsibility for the design, deployment, management, coordination, and operation of the campus wireless network infrastructure including 802.11 and related and future wireless network technologies and the use of frequencies that can, do, or have the potential to interfere with the performance or operation of the wireless network on the Colorado School of Mines campus to Academic Computing and Networking (AC&N). This authority and responsibility is designated to AC&N in order to ensure appropriate technical coordination and management of the infrastructure that is used to deliver services that use these technologies.

Rationale

While 802.11 and related wireless technologies are easy to deploy, they are sensitive to interference from overlapping frequencies. There are three non-overlapping channels available in the 802.11 air space. To most effectively create a seamless wireless network with maximum bandwidth, careful planning and network design is necessary, so technical coordination and central management is required.

Connecting wireless devices to the campus network has significant implications for network security. Since wireless devices provide network access to those connecting through the device, it is important that each device/user connecting to the network authenticate with the network. In addition, incorrectly configured wireless access points cause problems for network operation or performance in a variety of ways, such as providing invalid services (for example, a DHCP server providing invalid IP addresses.)

Scope

This Wireless Policy provides guidelines and requirements for the following:

1. Deployment of 802.11 and related wireless standards access points
2. Management of 802.11 and related wireless technologies
3. Deployment of any devices operating at frequencies that are determined to interfere with the operation or performance of the campus wireless network.

Policy

1. Academic Computing and Networking has the sole authority for designing, implementing, and operating all 802.11 and related wireless network infrastructure for the campus.
 - a. AC&N is responsible for the deployment and management of 802.11 and related wireless standards access points on the campus.
 - b. AC&N recognizes that the CSM Telecommunications Department operates the Companion wireless phone service in the 1.92 to 1.93 Ghz range. AC&N will work with Telecommunications to maintain current services and deploy future wireless voice services.
 - c. No department, student group, individual, or organization may install or deploy any 802.11 or related wireless standards access points on the CSM campus (including campus housing) without coordination through and approval from AC&N networking staff.
 - d. No department, student group, individual, or organization may install or deploy any device or service on the CSM campus (including campus housing) that does, or has the potential, to interfere with the campus wireless network infrastructure

managed by AC&N without coordination through and approval from AC&N networking staff. This includes devices that are not attached to the campus network but may interfere with wireless access points managed by AC&N.

2. Only individuals authorized by CSM through Academic Computing & Networking may use the campus wireless network.
3. Academic Computing and Networking will offer a standard wireless deployment plan that is expected to meet the needs of most departments, student groups, individuals, or campus organizations that wish to use wireless services.
 - a. Departments or campus organizations requiring a different wireless deployment plan (for technical reasons) may contact AC&N to request that AC&N construct and operate, if feasible, a premium wireless service to accommodate their special technical needs. Lower-cost wireless access points are not an acceptable reason for an alternate deployment plan. Departments must contract with AC&N for the purchase, implementation and maintenance of any approved alternate wireless deployment.
4. Academic Computing and Networking will manage all network-attached and 802.11 and related wireless standards access points.
 - a. AC&N will ensure that all wireless services deployed on campus will adhere to campus-wide standards for access control.
 - b. AC&N will manage the wireless spectrum in a manner that ensures the greatest interoperability and roaming ability for all individuals wishing to use the wireless technology.
 - c. AC&N will centralize the process of authentication and security for wireless users.
5. Academic Computing and Networking is authorized to disconnect and remove, without warning, any unauthorized wireless access devices it discovers that are attached to the CSM network.
6. Academic Computing and Networking is authorized to direct a department, student group, organization, or individual to remove or disable any device not previously approved by AC&N that is not attached to the campus network that is determined to be interfering with the operation or performance of the campus wireless network.

Procedures

Any department, organization, or individual wishing to deploy wireless technology where it is not already provided must contact AC&N networking staff by sending a request via email to network@mines.edu. AC&N will evaluate the request and work with the department, organization, or individual to develop a plan for purchase, implementation, and management.

Policy Enforcement

1. AC&N may, without warning, deactivate, disconnect, and/or remove unauthorized network devices of any kind, including wireless access points if they are connected to the campus network or if they are not connected to the campus network but are determined to be interfering with the operation of the campus wireless network.
2. AC&N is charged with monitoring and enforcing the provisions of this policy.
3. Appeals regarding decisions or enforcement actions should be directed to the Vice President for Academic Affairs.