



Colorado Department
of Public Health
and Environment

Wireless Security Guidelines

Action	Risk	Guidance
Individual accesses department systems and e-mail either from home, hotel, airport or Internet Café via a wireless Internet connection while using a department-issued laptop.	A hacker could “sniff” traffic if a department Virtual Private Network connection is not used. Also, if the operating system of the laptop is not patched, a hacker could install a backdoor Trojan, which could be used at a later time to report keystrokes and/or other information from the hard drive back to the attacker.	Use the Virtual Private Network client for encrypting information over the network and the Internet. Remove sensitive information from the laptop drive or encrypt it.
Individual starts a laptop configured with wireless access within the radius of other wireless access points. The user may not even know that laptop is configured for wireless access.	Some laptops look for wireless connections at startup, regardless of whether the user asked to do so or logged onto any network. A hacker might get access to the laptop and install a backdoor Trojan on an operating system that was not patched or that did not have antivirus protection.	Change the default operating-system settings in the laptops to disable automatic connections to wireless access points.
Individual installs a personal wireless access point for connecting to peripherals in the department, and s/he uses it while logged onto a department network.	This action may allow an outside “sniffer” to access the network, even though the wireless access point is not used to log onto the network.	At the department, ban all wireless access at points except those set up by OIT and installed with certain safeguards.
Individual uses a personal laptop, while away on department business, to check e-mail and perhaps to update a department information system. Laptop is configured for wireless access. No work has been done to harden the personal PC for wireless.	A hacker could “sniff” traffic, if a department Virtual Private Network connection is not used. Further, if the operating system of the laptop is not patched, a hacker could install a backdoor Trojan, which could be used at a later time to report keystrokes and/or other information from the hard drive back to the attacker.	Configure the laptop not to automatically search for wireless access points. Use a department Virtual Private Network for Internet access. Have a personal firewall and anti-virus software installed and updated. Finally, make certain that operating system patches/hot fixes are up to date.
Individual sets up a wireless access point at the department to provide wire access to a program information system. S/he does not work with OIT on technical safeguards for wireless installation.	This action may allow a “sniffer” to gain access to the department’s network and systems through the computer of a user who is accessing the wireless connection and is logged onto the network.	OIT shall approve all wireless access points and ensure that they are set up in accordance with department technical standards.