

Minnesota State Colleges and Universities

ITS Standard 5.23.A.

Security of Wireless Access Points and Wireless Local Area Networks

Part 1. Purpose.

This standard establishes responsibilities for appropriate use of wireless local area network (WLAN) technologies within Minnesota State Colleges and Universities. Only wireless systems that meet the criteria of this standard are approved for connectivity in college or university networks. The use of Minnesota State Colleges and Universities information technology is a privilege conditioned on compliance with Policy 5.22 and X.XX (insert security policy number), this standard and any procedures or guidelines adopted pursuant to this standard.

Nothing in this standard shall be interpreted to expand, diminish or alter the academic freedom provided under Board policy, a system collective bargaining agreement, the terms of any charter establishing a System library as a community or public library, or the Acceptable Use of Computers and Information Technology Resources policy 5.22.

Part 2. Applicability.

This standard applies to all users of System wireless local area networks, whether or not the user is affiliated with Minnesota State Colleges and Universities, and to all uses of those resources, wherever located.

Part 3. Definitions.

Subpart A. College or university. College or university, except where specified otherwise, means a System college or university, the Office of the Chancellor, or the Minnesota State Colleges and Universities System.

Subpart B. Security measures. Security measures means processes, software, and hardware used by system and network administrators to protect the confidentiality, integrity, and availability of the computer resources and data owned by the System or its authorized users.

Subpart C. System. System means the Board of Trustees, the Office of the Chancellor, the state colleges and universities, and any part or combination thereof.

Subpart D. Information Resources. Information resources means all data collected, created, received, maintained or disseminated by any Minnesota State Colleges and Universities user, regardless of its form, storage media or conditions of use.

Subpart E. Wireless Local Area Networks. A WLAN utilizes electromagnetic waves, particularly spread-spectrum technology based on radio waves, to transfer information between devices in a limited area.

Subpart F. User. User means any individual, including, but not limited to, students,

administrators, faculty, other employees, volunteers, and other authorized individuals using System information technology in any manner, whether or not the user is affiliated with Minnesota State Colleges and Universities.

Subpart G. Integrity. Integrity means assuring that information is kept intact, and not lost, damaged or modified.

Subpart H. Availability. Availability means assuring that information is accessible to authorized user as required.

Subpart I. Confidentiality. Confidentiality means assuring that information is accessible only as authorized.

Subpart J. Private Network. Private networks are those networks that may provide access to non-public data and information resources.

Subpart K. Public Network. A public wireless local area network is any network that allows public or unauthenticated use.

Subpart L. Special Network. A special WLAN are defined as any wireless network designed for a particular purpose other than allowing wireless access to the network. These networks typically use specialized client devices, are built for individual applications and do not allow general user access (e.g., inventory picking systems and wireless projection systems).

Subpart M. Must. This word indicates a statement that is an absolute requirement for a compliant implementation.

Subpart N. Must Not. This phrase indicates a statement that is an absolute prohibition for a compliant implementation.

Subpart O. Should. When the word “should” is used, the statement is recommended, but not required.

Subpart P. Should Not. The phrase “should not” is used in statements of practices that are not recommended, but which may be followed if circumstances warrant.

Subpart Q. May. The word “may” means that an item is completely optional.

Part 4. Responsibilities of All Users.

Subpart A. General.

1. A WLAN with access to non-public data must be segmented and configured as private networks.
2. No unauthorized wireless devices may be directly or indirectly connected to system networks. All wireless connections must be approved by a designated Information Technology security official and meet all requirements of this standard.
3. All system entities must have processes in place for the detection, location and removal of unauthorized wireless devices.
4. All system entities must have processes in place for monitoring and logging of

wireless local area networks.

Subpart B. Private Networks.

1. A private WLAN must require strong encryption.
2. A private WLAN must require per-user authentication and authorization.
3. A private WLAN may use strong or two-factor authentication: a combination of something the user knows (e.g., a password), and something the user has (e.g., a token card, fingerprint, etc.).
4. Traffic from a private WLAN and other private networks should be controlled by traffic filters. This traffic filter should also deny all traffic initiated into to the private wireless network.
5. A client connecting to private WLAN must verify the authenticity of the WLAN.
6. Any access point physically connected to a private wired network must be physically secured to reduce the risk of theft, modification, unauthorized access to private data and other information resources.

Subpart C. Public Networks.

1. A public WLAN must not allow access to any non-public data or to any information resource that is not accessible via an unauthenticated internet connection.
2. A public WLAN may allow unauthenticated use. However, authentication for access is recommended.
3. Traffic between a public WLAN and a private network must be controlled by a traffic filter that is configured with a default-deny policy. This traffic filter must also deny all traffic initiated into the public wireless network.
4. Any access point that is physically connected only to public wired networks should be physically secured to reduce the risk of theft and access to private data.

Subpart D. Special Networks.

1. A special WLAN should meet the requirements for a private WLAN if possible. If the client supports technologies appropriate for a private WLAN, those mechanisms should be used and the network should be defined as another private network.
2. Traffic between a special WLAN and a private network must be controlled by a traffic filter that is configured with a default-deny policy. This traffic filter must also deny all traffic initiated into to the public wireless network.
3. A special WLAN should be logically and physically separate from the rest of the network if possible.
4. A special WLAN should use the strongest authentication and encryption feasible.

Date of Implementation: January 1, 2007
Date of Adoption: July 19, 2006
Related Documents: Board Policy 5.23, Information Security
Date and Subject of Revisions: