

Minnesota State Colleges and Universities

ITS Standard 5.23.D.

Network Segmentation

Part 1. Purpose.

This standard establishes responsibilities for network segmentation within Minnesota State Colleges and Universities. To assist in the protection of our data, servers and other network equipment, we must segment our networks.

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

Part 2. Applicability.

This standard applies to all users of System technology resources, 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. System. System means the Board of Trustees, the Office of the Chancellor, the state colleges and universities, and any part or combination there of.

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

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

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

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

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

Subpart I. Special Network. Special networks are defined as any network designed for a particular purpose other than allowing access to other networks. These networks

typically use specialized client devices, are built for individual applications and do not allow general user access (e.g., inventory picking systems, HVAC and projection systems).

Subpart J. User Network. Networks that contain authenticated client devices.

Subpart K. DMZ Network. Networks containing filtered anonymously accessible servers.

Subpart L. Inside Network. Networks containing servers with non-public data that is isolated completely from public networks and is filtered from all other networks.

Subpart M. Management Network. Networks containing network infrastructure.

Part 4. Responsibilities of system information technology personnel.

Public Networks:

1. Unencrypted non-public data must not be stored on or transported over a public network.
2. A college or university managed firewall must exist between a public network and other network types.
3. Public networks must not contain college or university managed servers.

User Networks:

1. Multiple user networks may be defined.
2. Filters must exist between a user network and other networks.
3. User networks must not contain publicly accessible servers.
4. Inbound connections initiated from a public network to a user network must be prohibited.
5. Access to user networks should be authenticated.

DMZ Networks:

1. Multiple DMZ networks may be defined.
2. Filters must exist between a DMZ network and other networks.
3. DMZ networks must not contain user client devices.
4. DMZ networks may contain management client devices.
5. DMZ networks must not contain devices that store unencrypted non-public data.
6. Filters should exist between devices within the DMZ network.

INSIDE Networks:

1. Multiple inside networks may be defined.

2. Filters must exist between an inside network and other networks.
3. Inside networks must not contain user client devices.
4. Inside networks may contain management client devices.
5. Filters may exist between devices within the inside network.

MANAGEMENT Networks:

1. Filters must exist between a management network and other networks.
2. Management networks must not contain user client devices.
3. Management networks may contain management client devices.
4. Filters may exist between devices within the management network.

Network Access Grid:

1. Firewall filters between network segments are required.
2. Firewall filters are defined as:

	To -->	Public	User	DMZ	Inside	Management
From						
Public		Any	None	Specific	None	None
DMZ		Specific	None	Specific	Specific	Mgmt
Inside		None	Specific	Specific	Specific	Mgmt
User		General	Specific	Specific	Specific	Mgmt
Mgmt		none	Specific	Specific	Specific	Specific

General:

1. Generally open. Restricted on certain ports/protocols because of worms, viruses, etc.

Specific:

1. Default rule is 'deny all'
2. Open only on specific ports and protocols.
3. Must have supporting documentation.
4. Must be based on documented business needs.
5. Must be specific IP address and/or ports on server side connection. No port ranges or 'any'.

None:

1. Access is prohibited.

Mgmt:

1. Access is logged and trap protocols to management devices only.

Exceptions

Each college or university must have a process in place for documenting any exceptions from this standard.

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: