

Remote Access Policy

Background & Purpose

The policy defines standards for connecting to University of Wisconsin Superior's network from remote devices. These standards minimize the potential exposure to University of Wisconsin Superior from damages that may result from unauthorized use of its resources. Damages include the loss of sensitive or company confidential data or intellectual property, damage to public image, damage to critical University of Wisconsin Superior internal systems, etc.

Constraints

This policy applies to anyone accessing University of Wisconsin Superior network resources from non-University networks. This policy covers remote access not explicitly allowed through the campus firewall includes, but is not limited to: ResHall network connections, dialup modems, DSL, VPN, SSH, Wireless Access Points and cable modems, etc.

Definitions

Term	Definition
Cable Modem	Cable companies provide Internet access in their service areas over cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.
Anti-virus software	UW Superior requires Symantec anti-virus software to protect computers from malicious software
Operating System Patches	Client operating systems must be patch current as protect computers from malicious software
Blue Socket	Wireless authentication system governing network access for wireless devices.
Remote Access	Any access to a private network through a non-private network, device, or medium.
Clean Access	Quarantine for Res Life Student Owned computers to insure they are patch current, virus free and have anti-virus software
VPN	Virtual private networking enables secure private network via a public network such as the Internet using "tunneling" technology.
DSL	Digital Subscriber Line is a broadband Internet access technology that works over standard phone lines.

Policy Statements

1. Remote access privileges to University of Wisconsin Superior's network must be given the same consideration as an on-site connection to University of Wisconsin Superior.
2. Remote access to the Internet through the University network will be permitted for users conducting University business. Remote access users are responsible to ensure that family members do not violate any University of Wisconsin Superior policies, perform illegal activities, or use the access for outside business interests. Remote access users bear responsibility for the consequences should the access be misused. Please review the University technology policies for details of protecting information when accessing the University network remotely.
<http://www.uwsuper.edu/technology/Policies/>

Policy Procedures

1. All external access to networks, systems and data should be done through a centrally administered, tested and sanctioned remote access solution. This policy prohibits the establishment of any unauthorized inroads to the campus network. Any discovered mechanisms of this sort will be removed immediately.
2. Non-standard hardware configurations must be approved by Network Services. Network Services must approve security configurations for access to hardware.
3. All equipment remotely connected to University network, including PCs, must use up-to-date anti-virus software, operating system patches and must be virus free.
4. University of Wisconsin Superior provides secure remote access to the University network with authentication and encryption. Never provide your login or credentials to anyone, not even family members. For information on creating a strong passwords see the Password Policy.
5. Students in the Residence Halls wanting to connect personally owned systems to the campus network may do so by authenticating through Clean Access and passing it's security requirements.
6. Wireless clients may access the campus network by authenticating through Blue Socket and passing it's security requirements
7. Faculty and Staff wanting to access the campus network remotely using a non-University computer may do so using a remote control application into their work computer.
8. Faculty and Staff wanting to access the campus network remotely using a University computer may do so using a VPN connection.
9. Dialup access to the campus network is not permitted.

Compliance

Any employee violating this policy may be subject to disciplinary action, up to and including termination of employment.