

## Montana State University ResNet Wired and Wireless Acceptable Use Policy

Montana State University provides a residential network (ResNet) to its Residence Halls and Family/Graduate Housing for educational, instructional, and entertainment purposes. It is the responsibility of each student and/or family to use these services appropriately and in compliance with all University, City, County, State, and Federal laws and regulations. MSU ResNet reserves the right to restrict access and enforce the terms of this agreement.

1. ResNet services (wired or wireless connections) are for the use of MSU residents only. The registered user is responsible for any and all activity that occurs on both the wired and wireless connections registered to them.
2. ResNet Wireless is a convenience network, available only in the residence halls. The wired connection in your room is faster, more stable, and more secure. ResNet Wireless is open, with no encryption. Be aware of the type of data you may be transmitting over the air waves.
3. Falsifying ResNet registration information will result in the temporary or permanent loss of ResNet services, with a possible referral to the Office of Student Affairs for disciplinary action.
4. The use of any type of wireless equipment including but not limited to wireless switches, wireless routers and wireless hubs in the Residence Halls is prohibited. Wireless routers used in Family and Graduate Housing must be secured.
5. The use of a hub or router on ResNet is prohibited. Permission to use a switch on ResNet must be approved prior to the use of the switch and will be evaluated on a case-by-case basis by the ResNet administration. The use of a network switch could be subject to an additional connection fee. Users are prohibited from using a switch or other device to provide a ResNet connection to any other person.
6. The residential network is a shared resource. Consequently, network uses or applications that use excessive bandwidth or otherwise inhibit or interfere with the use of the wired or wireless network by others are not permitted. Bandwidth usage limits are enforced as a total amount of data transferred in a 24-hour period.
7. ResNet reserves the right to immediately disconnect any computer temporarily if the computer is found to contain viruses or Trojan horse software in order to protect the network. It is the responsibility of the user to make sure their computer has current virus protection software installed and operational. The user's ResNet connection will be restored when it has been determined that the user's computer is completely free of viruses and is running current virus protection software.
8. All network-shared devices, drives and directories **must** be password protected to limit access to those whom the user authorizes and also to prevent the spread of viruses.
9. Users shall abide by all applicable copyright laws and licenses. The ResNet network may only be used for legal purposes and to access only those systems, software and data that the user is authorized to use. Sharing access to copyrighted software or other copyrighted materials (including MP3 files from copyrighted music media and digitized video from copyrighted motion pictures, etc.) is prohibited unless specifically authorized by the copyright holder. Please see MSU's "Copyright Infringement Disclosure" on the MSU Student Success website and MSU's "Copyright Infringement Prevention Plan" at <http://www.montana.edu/itcenter/policy/> for more information about the consequences of copyright infringement at MSU.
10. Commercial or for-profit use of ResNet or MSUNet is prohibited.
11. ResNet may not be used to provide Internet or MSU network access to anyone other than the ResNet customer for any purpose.
12. Any user who circumvents/defeats or attempts to circumvent/defeat the ResNet firewall or any other mechanism put in place by ResNet to manage the network will be subject to immediate termination of service and possible disciplinary action.
13. ResNet network services and wiring may not be modified or extended by users for any purpose. This applies to all network wiring, hardware, data jacks and wireless access points.
14. Costs to repair physical damage to the ResNet hardware in the room or apartment (including wiring, data jack, conduit or box, wireless access points) will be assessed to the resident.
15. Use of connected networks, including MSUNET, the Internet, and Internet2 must be consistent with the rules and acceptable use policies established for those networks by their providers. (MSUNET AUP: [http://www2.montana.edu/policy/computing\\_manual/comp400.html#410.00](http://www2.montana.edu/policy/computing_manual/comp400.html#410.00)).
16. The provision of network services from user computers (e.g., HTTP, Peer-to-peer apps, Chat, DHCP, DNS, FTP, IRC, NNTP, POP3, SMTP, Telnet, WINS, etc.) is prohibited.
17. Use of ResNet implies user's consent for ResNet administration or its agents to monitor activities, traffic, and data via the user's data connection for the purpose of determining compliance with this agreement.
18. It is up to the user to make their computer and data safe from other users on the network; the user will not hold MSU-Bozeman liable for malicious acts by other network users.
19. If you have a reason to believe that another user or group of users is interfering with your access to the network, you may report the problem to the ResNet office and expect that the ResNet administrators will investigate and if necessary take corrective action. (ResNet Center phone: (406) 994-1929; email: [resnet@montana.edu](mailto:resnet@montana.edu)).
20. Any unauthorized attempt to access another computer or device (on or off campus) is prohibited. Any reports received by the ResNet administration of unauthorized attempts to access other connected devices will result in the immediate disconnection of the suspected network connection until the matter has been resolved. Some examples of unauthorized attempts to access are password cracking programs, port scanning any device that is not owned by the person doing the

scanning, gaining access or attempting to gain access to another connected device without the owners' permission, and capturing/sniffing wireless packets.

21. ResNet reserves the right to immediately disconnect any computer or device that is sending disruptive signals to the network, whether because of a defective cable, Ethernet card, or other hardware or software problem. It will be the user's responsibility to correct any such problem before the computer can be reconnected to ResNet.
22. ResNet reserves the right to immediately disconnect any/all network-connected devices temporarily for the purpose of network hardware, software, security troubleshooting, or for network maintenance, or to enforce the ResNet Acceptable Use Policy.

## **AUP Enforcement**

Consequences for AUP violations, per offense type:

- 1<sup>st</sup> Offense: Warning
- 2<sup>nd</sup> Offense: Three day suspension of service
- 3<sup>rd</sup> Offense: One week suspension of service
- 4<sup>th</sup> Offense: Service suspended indefinitely until a mutual resolution is found between ResNet, Dean of Students and the offender.

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by ResNet administration. This may be done through voice or e-mail, or in-person discussion and education. ResNet also runs a full service help desk where we can assist in virus cleaning, system security configuration, etc.

Repeated minor infractions or misconduct that is more serious will result in the temporary or permanent loss of ResNet access privileges, or the modification of those privileges. For example, multiple offenses will result in longer periods of service disconnection. More serious violations include (but are not limited to) unauthorized use or distribution of computer resources, repeated virus infections, repeated bandwidth offenses, repeated file sharing violations, repeated wireless offenses, attempts to steal passwords or data, unauthorized use or distribution of copyrighted materials, harassment or threatening behavior. In addition, offenders may be referred to their sponsoring advisor, department, or other appropriate University office for further action. If the user is a student, the matter may be referred to the Office of Student Affairs for disciplinary action.

ResNet may require that the user bring their computer or electronic equipment to our help desk center in order to verify compliance with this acceptable use policy before service is restored.

Any action that violates local, state, or federal laws may result in the immediate loss of ResNet access privileges and will be referred to the appropriate University offices and/or law enforcement authorities.