MONTANA STATE UNIVERSITY NORTHERN

ResNet Acceptable Use Policy

MSU-Northern Information Technology Services provides a residential network (ResNet) to its Residence Hall for educational, instructional, and entertainment purposes. Use of these services is a privilege. It is the responsibility of each student to use these services appropriately and responsibly in compliance with all University, City, County, State, and Federal laws and regulations. This policy is in addition to MSU-Northern and MUS Board of Regent policies which include, but are not limited to, student conduct and those that prohibit harassment, discrimination, etc. MSU-Northern ResNet reserves the right to restrict access, availability of access, and enforce the terms of this agreement. Connecting to a ResNet data, voice, or cable TV services signals your FULL agreement and understanding of this Acceptable Use Policy and any future modifications thereto.

1. Use of connected networks and the Internet must be consistent with the rules and acceptable use policies established for those networks by their providers.

2. 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 copy-righted 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 copyright holder.

3. The residential network is a shared resource. Consequentially, network uses or applications that use excessive bandwidth or otherwise inhibit or interfere with the use of the network by others are not permitted.

4. In order to help protect the University network against computer viruses, worms and Trojan horse programs that can cause damage or pirate information each computer connected to the ResNet network must have McAfee anti-virus software installed, and this will be provided to you at no cost.

5. Forgery or other misrepresentation of one's identity via e-mail or any other form of communication is a violation of University policy. This includes forging of IP addresses and/or NIC addresses to conceal your computer's identity and the use of forged or false identity when using certain e-mail

programs (i.e. pop-mail clients such as Eudora, Netscape, Outlook, Outlook Express, etc) and is grounds for losing your campus network privileges.

6. ResNet may not be used to provide Internet or MSU-Northern network access to anyone outside of the ResNet community for any purpose.

7. The provision of network services from user computers (e.g., HTTP, BBS, Chat, DHCP, DNS, FTP, IRC, NNTP, POP2/POP3, SMTP, Telnet, WINS, etc.) is prohibited.

8. Commercial or for-profit use of ResNet access is prohibited.

9. Any user who attempts to circumvent or 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.

10. Any unauthorized attempt to access another computer (on or off campus) is prohibited. Any reports received by the ResNet administration of unauthorized attempts to access other computers 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 computer that is not owned by the person doing the scanning, and gaining access or attempting to gain access to another computer without the owners' permission.

11. Users are ultimately responsible for the security and integrity of their systems, data and all traffic originating from their computer. ResNet users will not hold MSU-Northern liable for malicious acts by other network users.

12. ResNet services and wiring may not be modified or extended by users for any purpose. This applies to all wireless and cabled wiring, hardware, data jacks, related hardware and network or Internet services. Hubs, mini-hubs, remote access servers and/or any equipment that may change the network topology or deny others service are not allowed on ResNet.

13. Costs to repair physical damage to the ResNet hardware in the room or apartment (including wiring, data jack, conduit or box) will be assessed to the resident.

14. Only one IP address will be assigned to each registered computer. Residents may not have multiple IP addresses per computer. Only one computer may be registered to each individual student at any given time.

15. Residents understand that the network extended to student rooms is the property of the University and that the campus network administrators monitor and inspect network traffic for the purposes of assuring the proper

operation of the network, fair allocation of resources, and for other lawful purposes. There is no expectation of privacy in the use of this University resource.

16. Use of ResNet implies user's consent for ResNet administration or its agents to monitor activities/traffic via the user's data connection for the purpose of determining compliance with this agreement.

17. ResNet reserves the right to immediately disconnect any computer that is sending disruptive signals to the network as a whole, 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.

18. 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 ITS Help Desk ext. 3765 and expect that the ITS network administrators will investigate and if necessary take corrective action.

ResNet reserves the right to modify, change and reformat this document as it deems necessary without permission or consent of its network users.

AUP Enforcement

The Information Technology Services (ITS) administrators may temporarily suspend network privileges of any ResNet user while suspected violations are being investigated or adjudicated, even if it affects network services of roommates. Sanctions as a result of violations of these regulations may result in the following:

- Suspension of revocation of ResNet privileges;
- University sanctions prescribed by student behavioral codes;
- Reassignment, contract jeopardy, revocation of license, or eviction from University housing and/or the University;
- Prosecution under applicable state and/or federal civil or criminal laws.

Minor infractions of this policy, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by ITS administration. This may be done through voice or e-mail, or in-person discussion and education.

Repeated minor infractions or misconduct that is more serious may result in the temporary or permanent loss of ResNet access privileges, or the modification of those privileges. More serious violations include, but are not limited to, unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or distribution of copyrighted materials, repeated harassment or threatening behavior. Offenders may be referred to their advisor, department, or 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.

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

In the case of disconnection due to suspected use violations, the user can expect that the ITS administration will make every effort for a speedy resolution (in most cases, within 3 business days) and resumption of service if appropriate.

ResNet reserves the right to modify, change and reformat this document as it deems necessary without permission or consent of its network users.