ATM Unix System Acceptable Use Policy

1. All SDSM&T Policies apply to the ATM user policies. Logging onto any console or network affiliated with SDSM&T binds you to these policies. It is your responsibility to read them and comply with them. These policies can be found at these include the BOR Acceptable Computer Use Policy: http://its.sdsmt.edu/docs/110905.pdf and the SDSMT's AUP agreement: http://www.sdsmt.edu/Campus-Services/ITS/How-Do-I/SDSMT-Computer-Use-Policy/

2. All research and coursework using our computing system also automatically binds you to the SDSM&T Academic Integrity Policy as stated in the University Catalog.

3. ATM Students and Staff whose projects and coursework require a Unix computer account should be issued one by the lead PI (research) or Lead Professor (coursework). The level of access will be determined at the faculty level. These accounts are separate from the SDSM&T account system but are bound by the same policies.

4. All computing access is provisional to compliance with SDSM&T and ATM policies. Violating AUP may result in revocation of computer access regardless of your academic or research obligations. ATM is NOT obligated to provide computing resources to anyone.

5. USERS WILL NOT RELEASE USERNAMES OR PASSWORDS TO ANYONE!

6. Students should neither be given nor request root or superuser privileges.

7. The student's technology point-of-contact is the course professor or project advisor.

8. Projects requiring excessive disk space (e.g., over 1 TB) must get prior approval from both Drs. Detwiler and Capehart.

9. ALL STUDENTS USING THEIR OWN SYSTEMS (E.G., LAPTOPS) ON THE SDSM&T NETWORK ARE EXPECTED TO HAVE AND MAINTAIN UP-TO-DATE COMPUTER VIRUS SOFTWARE, STRONG SECURE PASSWORDS AND INACTIVITY LOCK OUTS.

10. Remote Access to the UNIX network is available through department-approved software. For access from Windows machines, this includes Putty, SSH and Xming.

11. ALL Users are expected to maintain their accounts and SDSM&T/ATM IT resources in a professional, mutually productive, legal and ethical manner. Users are expected to maintain and develop their Unix competency. Users will be mindful of their use of disk and RAID space. Filling a drive can disrupt scheduled Unix tasks and your colleagues’ research and classwork. LUSER™ management will be swift and merciless.

12. NO FOOD OR DRINK AT CONSOLES. Consoles are not private workspaces. Respect project-restricted workstations.

13. Do not leave sessions on public machines unattended and unsecured. Unattended consoles will lock out other users. In these cases Management will intervene with no regard for the work being done on the console in the users absence.

14. Maintain building security. DO lock doors leading into ATM infrastructure during off-hours. This includes the outside doors.

15. Do not attempt to "fix" any problem on the system. Bring these to the attention of your supervisor immediately. Provide all details. "My stuff doesn't work," or "Something's making funny noises" is insufficient.