Administrator Agreement

Please print:

Hostname: _________________Location:______________________________________

Name: ________________Email address: ________________Phone: _______________

Date: ________________ Operating System & Version: __________________________

As a computer administrator you are assuming the responsibility for maintaining the system in a secure fashion according to the policy outlined in this document. A computer administrator is required to abide by the following rules, which are subject to change.

1. Strictly adhere to the University of Missouri Acceptable Use Policy posted on the web at: http://www.umsystem.edu/ums/departments/gc/rules/facilities/110/005.shtml and the Missouri S&T Acceptable Use Policy posted at: http://it.mst.edu/policies/index.html.
2. Shall not connect any equipment to the campus network without coordination with IT.
3. Shall not permit any network intrusion/scanning/other tools to make connections from the system to other systems on the network without the consent of the administrator of the other machine. Normal service access connections to published services are permitted.
4. Shall not add any services exposed to the network to the computer without coordination with IT.
5. Shall not permit any cleartext authentication services to be enabled on the machine. For example, this includes but is not limited to telnet, ftp, xdm, rsh, rlogin, rexec and web authentication. That means kerberized-telnet, ssh, and sftp are required, and any web based authentication must be either done with javascript encrypted data or via SSL.
6. Shall obtain SSL certificates for the computer through IT.
7. Shall not run any network data capture (sniffer) software, or other tools, except when such tools are limited to diagnostics of service activity related to this system only.
8. Shall not permit the computer or any service on it to be used as a means to circumvent any limitation imposed by IT network security or policies. Example: Running SSH on a non-standard port to get around the firewall. Example: Running a proxy server.
9. Shall be responsible for maintaining patch currency as specified by IT and monitoring network security lists and advisories for any issues. If the operating system is being maintained by IT, then IT is responsible for patch currency on standard install components.
10. Shall maintain an administrator contact for the system at all times. For any time that no contact will be available the system must be shut down.
11. Shall disable any service deemed by IT to be a hazard to the campus network security or stability.
12. Shall not permit any sensitive information to be stored on the machine without special arrangements coordinated through IT. Example: credit cards, social security numbers, medical data.
13. Backups are the administrator's responsibility unless coordinated through IT.

When the system is to be partially maintained by IT, such as with a Missouri S&T standard RedHat UNIX or Windows XP install, the following additional rules are to be followed:

1. Shall not make any changes to automatically maintained facilities such as root's cron configuration, password file, and kerberos and ssh services, SUS, etc.
2. Shall remove any changes made that are deemed by IT to be incompatible with our environment or base installation.

All changes to the system shall be coordinated with an IT representative designated for the project. The expectation is that if you are going to do something new/different with the machine, it will be done under IT direction. Where appropriate, that representative will designate ranges of activities that can be performed without additional coordination or direction of IT.

IT will not be held responsible for the functionality of the machine or services you provide on it. This shall include data stored on the system unless coordinated with IT. In the case of systems using our standard install, we will take responsibility for the functionality provided by our base install.

IT will actively monitor the system to ensure compliance is maintained.

These rules are vigorously enforced. Violation may result in a denial of access to University computer resources, and having userids restricted, revoked or access curtailed. In addition, research assistantship funding may be revoked. Certain cases of abuse may also result in prosecution, termination, or academic probation.

This agreement shall be renewed annually.

Disciplinary Action

Misuse of University computing facilities will be reported to the Vice Chancellor of Student Affairs, the Provost, Human Resources or University Police, whichever is appropriate. Possible disciplinary actions for students are detailed in the Student Handbook and can include criminal prosecution under Missouri Law.

I, the undersigned, have read this policy and the University of Missouri Acceptable Use Policy and I agree to abide by these policies.

____________________________________ ______________________

Signature Date Signed

Advisor/Supervisor Name (print): _______________________________

____________________________________ ______________________

Advisor/Supervisor Signature Date Signed