

Special Access Guidelines Agreement

This agreement outlines the many do's and do not's of using special access accounts. Special access is defined as having the privilege and password to use domain administrator accounts. The Montana Tech environment is very complex and dynamic. People with special access must develop the proper skill for using that access responsibly. The Special Access Guidelines have been developed to help people to use their special access in a responsible and secure manner. All persons requesting special access must read and sign this agreement. Anyone refusing to sign this agreement will not be granted the special access that they requested.

1.0 General Guidelines

Documentation provides a method to analyze what happened. In the future, others may want to know what was done to correct a certain problem. The Lead System Analyst, Subsystem Manager or resource owner is to be informed BEFORE any changes are made to system specific or configuration files.

1.1 Be aware of the Montana Tech environment.

The Montana Tech facility is a highly specialized facility containing a large number of computers of different configurations. Many daily system tasks have been automated by the use of software tools. Be aware of the "MONTANA TECH Way" of doing system tasks.

1.2 Always log on systems with the least privilege to perform the task.

1.3 Use special access only if necessary.

Many system tasks require the use of root or other special access. However, there are many tasks that can be done without the use of special access. When at all possible use regular accounts for trouble-shooting and investigating.

1.4 Document all major actions and/or inform appropriate people.

1.5 Have a backup plan in case something goes wrong.

Special access has a large potential for doing damage with just a few keystrokes. Develop a backup plan in case something goes wrong. You must be able to restore the system to its state before the error occurred.

1.6 Know whom to turn to if problems arise.

With the use of special access, situations arise that have never come up before. Although MONTANA TECH has many written procedures, they do not cover every circumstance possible. If any doubt exists about how you should proceed on a problem, then ask for assistance. Know whom to ask.

2.0 Specific Do not's of Special Access

- **Do not share special access passwords with anyone!**

- **Do not write down the special access passwords or the current algorithm.**
- **Do not routinely log onto a system, as "root" or any other special access account.**
- **Do not read or send personal mail, play games, read the net news or edit personal files using a special access account.**
- **Do not browse other user's files, directories or E-mail using a special access account.**
- **Do not make a change on any system that is not directly related to your job duties.**

The CSA is responsible for approving all changes to the systems(s) of his/her responsibility. No changes are to be made to any system configuration file or executable file without prior approval of the Lead System Analyst". Making a change AND then informing the CSA is considered a violation of this guideline.

- **Do not use special access to create temporary files or directories for your own personal use.**

I certify that I have read the above guidelines and will use this special access in accordance with MONTANA TECH guidelines and policies. Misuse of any special access privilege will result in removal of that access.