System Security

These policies and procedures are intended to help you make the best use of the computer resources at your disposal. You should understand the following:

1. You are individually responsible for protecting the data and information in your hands. *Security is everyone's responsibility*.
2. Recognize which data is sensitive. If you do not know or are not sure, ask.
3. Even though you cannot touch it , information is an asset, sometimes a priceless asset.
4. Use the resources at your disposal only for the benefit of Nez Perce Tribe.
5. Understand that you are accountable for what *you* do on the system.
6. If you observe anything unusual, *tell your supervisor.*
7. All stations must be virus protected by antivirus scanning software, it is the employees responsibility to run live updates of the authorized and licensed anti virus software. Employee's should notify Information Systems if the anti virus protection software expires or is nonfunctional.

When using the Tribe's computer systems you should comply with the following guidelines:

DO's

1. Choose a password that consists of a mixture of at least 6 alphanumeric characters. Establish a screen saver password that coincides with your domain login password.
2. Log off before you leave your workstation, if you are working on sensitive information or leaving your workstation for any length of time.
3. Ask people their business in your area, if they look as though they do not belong there.
4. Protect equipment from theft and keep it away from food and drinks.
5. Ensure that all-important data is backed up regularly (weekly for critical data, monthly for all data). Consult with Information Systems if you require assistance.
6. Make sure that on every occasion that floppy disks and other media are brought in to the Tribe that they are checked for viruses before use.
7. Inform Information Systems immediately if you think your workstation may have a virus.
8. Report anything unusual to your supervisor.

DO NOT

1. Do not write down your password, do not share or disclose your password.
2. Do not give others the opportunity to look over your shoulder if you are working on something sensitive.
3. Do not use shareware (software downloaded from the Internet or on PC magazine covers).
4. Do not duplicate or copy software or audio CDs.
5. Do not install any software on your machine or alter its configuration, this work may only be undertaken by Information Systems.

Please note the following
Your PC will be audited periodically. Logins to, and use of the Tribe's network are audited and monitored.