ACOM Authenticator Security Acknowledgement Form

This form is required to use an authenticator in ACOM – that is, a password or a hardware token such as a YubiKey or CRYPTOcard. Please read and sign the following agreement & return to the senior System Administrator, Tim Fredrick (FL0-2112). Once this form is received, an authenticator may be issued. Remember that we all share a responsibility for IT security and to use reasonable precautions to prevent unauthorized access to ACOM information systems.

Hardware tokens (YubiKey or CRYPTOCard).

Hardware authentication tokens are used to generate single-use passwords in UCAR's computing environment. Please read the following and answer the first question. By signing this form, you are agreeing to the statements below:

- I am currently requesting or using a hardware authentication token: ___YES ___NO
- My token will remain in my custody and is for my use only and may not be shared.
- I will immediately report loss of custody of my hardware authentication token to my system administrator.
- My PIN number may not be shared or made available in unencrypted electronic form.

Passwords:

Passwords are issued bi-annually by ACOM, typically in April and October. While there are technical means to change from this password, the ACOM IT group strongly prefers that you use the assigned password. A form is available to generate and request a password at any time (http://www.acom.ucar.edu/help, following the link "Request new password" on that page).

By signing this form, you are agreeing to the statements below:

- System Administrators may have a copy of your password for use during troubleshooting. The password may not be disclosed outside of the IT group.
- Passwords must be changed every 6 months.
- I will not reuse an old password.
- I will not share my password or authenticator token with any other individual.
- I may keep the password in written form, but secured from access by other individuals. It will not be in a place viewable by electronic devices such as cameras.
- I will not keep my password in non-encrypted electronic form.
- I will not send my password by email, even to the IT group.
- I will immediately report to my system administrator known or suspected disclosure of my password. I will report to my system administrator any loss of custody of my authenticator token including loss or theft.

For questions or concerns about any of these points of agreement, please see your system administrator. By signing below, you indicate understanding and agreement as the ACOM lab strives to maintain a safe and secure computing environment.

Name (please print): _____

Signature: _____ Date: _____