



National Space Science and Technology Center University of Alabama in Huntsville

Network Equipment Registration Request

Network Information

Wireless & Visitor	Private	Public
<input type="checkbox"/> Wireless <input type="checkbox"/> Wired Expiration Date _____	-OR-	<input type="checkbox"/> Global <input type="checkbox"/> NAT * choose only one
	-OR-	<input type="checkbox"/> Global

System Information

Device	OS	Ownership
<input type="checkbox"/> Desktop <input type="checkbox"/> Laptop <input type="checkbox"/> Server/Rackmount <input type="checkbox"/> Other _____	<input type="checkbox"/> Windows <input type="checkbox"/> MacOS <input type="checkbox"/> Linux <input type="checkbox"/> Other _____	<input type="checkbox"/> UAH Tag ID _____ <input type="checkbox"/> NASA Tag ID _____ <input type="checkbox"/> Corporate <input type="checkbox"/> Personal

HOSTNAME _____ OS VER _____ LOCATION _____

WIRED ____ : ____ : ____ : ____ : ____ : ____ WIRELESS ____ : ____ : ____ : ____ : ____ : ____
 Please include MAC addresses for all interfaces in the system, even if they are not going to be used in this network.

I acknowledge that while I am using the NSSTC network, I must abide by the IT policies in this document.

 Machine Owner Signature and Date Print Name Phone

 UAH Responsible Official Signature and Date Print Name Phone
 Line Manager if NASA Owned

Administrator Security Checklist

<input type="checkbox"/> OS Patches Applied	<input type="checkbox"/> AD Domain Member	<input type="checkbox"/> Removed from Network Date _____
<input type="checkbox"/> Antivirus up-to-date	<input type="checkbox"/> Firewall Enabled	
<input type="checkbox"/> Antispyware Installed	<input type="checkbox"/> System Scanned	Security Plan _____

 IT Administrator Signature and Date Print Name



National Space Science and Technology Center University of Alabama in Huntsville

Network Equipment Registration Request

Policies

- Install Antivirus software and configure the software to update on a **daily** basis
- Install and keep up with the latest patches
Windows users can go to <http://windowsupdate.microsoft.com>
- Install Anti-spyware software
Windows users can download Windows Defender free from <http://microsoft.com>
- Enable the system firewall
- Disable services that are accessible without a password (web server , anonymous ftp server, shares, etc)
- Users will not undermine nor circumvent network and host security procedures.
- Users will take reasonable steps for protecting the integrity and privacy of this equipment as well as the information stored within.
- Users must follow the UAH General Computer Use Policy.

Legal Information

The NSSTC-UAH network is only to be used by authorized personnel. By accessing the network, you are consenting to system monitoring including the monitoring of keystrokes. It is your responsibility to take precautions to prevent others from gaining access to your account credentials. Unauthorized use or access to this network may subject you to criminal prosecution.

UAH General Computer Use Policy

You will:

1. Be accountable for using university facilities in an ethical and lawful manner.
2. Use only those facilities for which you have been authorized, whether facilities are at UAH or at any other location accessible through a network. You are required to adhere to the policies established by the administrator of local computing facilities at UAH and the University's Internet provider AREN (Alabama Research and Education Network. See: <http://www.asc.edu/html/accusepol.shtml>)
3. Take all reasonable steps to protect the integrity and privacy of the UAH computing facilities including software and data. In particular, you will not share with others the access codes, account numbers, passwords, or other authorization assigned to you.
4. Not use university facilities to access, download, print, store, forward, transmit or distribute obscene material.
5. Adhere to the copyright laws regarding software, data, and authored files.
6. Respect the privacy of others by refraining from any and all unauthorized access to e-mail, files, data, and transmissions.
7. Not use the UAH computing facilities for unauthorized commercial activities.
8. Not use the UAH computing facilities for any illegal purposes. Such acts include but are not limited to: accessing, destruction of, or alteration of data owned by others; modification of computer system configuration; installation of unauthorized software; interference with access to computing facilities or harassment of users of such facilities at UAH or harassment of users of such facilities elsewhere; unauthorized disruption of UAH computing facilities; attempts to discover or alter passwords or to subvert security systems in any computing or network facility.
9. Properly identify yourself in any electronic correspondence and provide valid, traceable identification if required by applications or servers within the UAH computing facilities or in establishing connections from the UAH computing facilities.