# United States Antarctic Program

## Computer Requirements For Connecting to the USAP Network

The United States Antarctic Program (USAP) addresses U.S. federal government security and operational requirements for computing systems by screening all computers (including science experiments, mission operation systems, workstations, PCs, servers, laptops, and portable notebooks) prior to connecting to the USAP network. The following system requirements and operating system specifications apply to all computing devices including iPhones, iPads, tablet devices and Personal Digital Assistance (PDA) that could connect to the USAP network. These requirements are aligned with the *NSF Computer Security Policy*. Please direct inquiries to the USAP Help Desk at (720)568-2001 or helpdesk@usap.gov.

To minimize wait time for computer screening, please ensure your system meets the following requirements prior to deployment. Failure to comply with the following guidelines may result in excessive delays or a denial of access. For more information on meeting USAP computer requirements see *How to Pass Computer Screening*.

**A computer system must continuously maintain compliance with these computer requirements. A system that falls out of compliance such as falling behind in anti-virus definitions, patches, or vulnerability remediation may be disconnected without notice, if the NSF determines there is an unacceptable level of risk or threat to the USAP environment.**

## System Requirements

- **Administrator Access**
  *Obtain administrator username and password for computers prior to deployment.*
  Screening technicians must have the authority to log on to the computer at an administrator level to accurately review the system configuration and run screening software. To maintain the security of your system it is recommended that you set a temporary administrator username and password for use during computer screening. If the administrator username and password are not available, the screening process, as well as the ability to connect to the USAP network and its resources, will be delayed.
- **Connectivity**
  Participants must provide all the equipment necessary to connect the computer system to the USAP network, including the Network Interface Card (NIC), external dongles or attachments used by the NIC, device drivers, etc. All equipment must be in working order.
- **Antivirus**
  All devices must have antivirus software running at the current version and be configured for auto-updates. Computers must be virus free prior to connecting to the USAP network and maintain the current DAT version as updates are available.
- **Operating System and Software Patches**
  Devices running an operating system (OS) must be running at a version currently supported by the vendor, and be updated with the most current patch level of the OS, including the latest security patches. Applications running on the system must also be patched when patches are released by the software vendor.

- **Client and Server Software and Data Transfer**
  - Client software used for the purposes of email and web browsing, and other client software, such as SSH and SFTP, are permitted.
  - Computers are not permitted to use insecure protocols such as Telnet for accessing systems or FTP for transferring data across the USAP network.
  - Software that is not permitted for use on the USAP network includes but not limited to:
    - Peer-to-peer (P2P) software, e.g., BitTorrent, KaZaA, Gnutella, Freenet
    - Email server software that provides SMTP/POP port services
    - Web server software that provides HTTP/HTTPS/FTP services
    - Network management servers, such as DNS and SNMP
    - Network or port scanning software, such as Nessus
    - Unauthorized wireless access points
  - Software requiring NSF approval for use on the USAP network for official business purposes (such as educational outreach) includes Skype and other video and audio streaming software.

If your system has embedded software or can only be patched when the vendor releases an update, notify USAP IT several months in advance of deployment to design your science support requests or mission support requests to receive a preliminary connection determination. The system will be evaluated to determine if it is secure, robust, and able to withstand continuous security, maintenance, and network management activities that occur on the USAP network.

## Computer Screening Process

Screening technicians gather the following information during the computer screening process. System operators who connect to the USAP network without a screening rating of *Pass* are in violation of USAP information security policy and may be disconnected without notice. A *Fail* rating indicates the system owner is responsible for remediating the system as soon as possible in order to remain connected to the USAP network.

| Data Collected By Computer Screening | |
|---|---|
| ▪ Computer make and model<br>▪ Computer hostname<br>▪ MAC address | ▪ Wireless MAC address<br>▪ OS version and patch level<br>▪ Antivirus software version and DAT file date |

Computer screening is performed at the following locations:

- Denver, Colorado
- Christchurch, New Zealand
- McMurdo, Palmer and South Pole Stations
- Marine Research Vessels (LMG and NBP)