COMMUNICATIONS and SHIPBOARD COMPUTING

VOICE

The communications capabilities aboard the Lake Guardian consists of marine VHF radio, Ku band maritime VSAT Internet system, a dedicated Cisco Unified Communications system's Voice over IP (VoIP), via the VSAT internet provider, which manages the external and internal voice communications as well as the shipboard paging system. In addition to VHF radio, a dedicated Iridium satellite phone service is deployed as a backup telecommunication system for emergencies in the event the VSAT system encounters disruptions while at sea. As an additional measure for safety, the Master is also equipped with a cellular smartphone for communications with shore when the vessel is within cellular range.

The pilot house is equipped with a dedicated VoIP line that is designated for the Master and Watch Officers to conduct their business while on duty on the bridge. There's a general VoIP phone line for the crew and other visiting scientists to use for voice communications to shore while on board the vessel. There is also a VoIP line that is used for the two designated EPA cabins that allow EPA staff to conduct business with their home offices. All berthing cabins, laboratories, lab office and lounge area are equipped with Cisco VoIP phones to allow personnel to make and receive calls anytime while on board.

Please contact the Master for the general phone number if you need or expect to receive incoming calls from shore for personal or business related activities. Incoming calls can be dialed directly to the cabins if callers are given the internal ship numbers. The list of the ship's internal numbers can be obtained from the Master, Mates or Marine Technicians.

SHIPBOARD COMPUTERS

The ship's computing capability consists of a 24x7 satellite Internet service, router, firewalls, switches, SAN and NAS devices for data storage, physical servers and virtual servers, which host Windows 2012 R2 servers for network domain access and database support. The ship is equipped with a wired and wireless Local Area Network (LAN) that supports Windows 7/8/10 Professional clients for running support and analytical applications.

There are three laptops located in the lab office for crew and visiting scientists to use to access email, Internet and network printing. The lab office also houses two networked printers for general use.

To access the Internet from available laptops, a network login id is required and can be requested through the Master or the Marine Technicians. Visiting scientists who bring their own laptops on board can connect to the ship wireless network for Internet access provided that the laptops must have an antiviral software installed and active scanning is enabled.

SHIPBOARD NETWORKS and POLICY

The ship has a fiber and copper LAN and a wireless network through-out the entire ship. The key to logon to the wireless network is written on the bottom of white board outside the lab office. Please make sure your laptop has antivirus software and has the latest virus pattern files. To conserve the bandwidth for official use, please DO NOT misuse the Internet. The Internet activities are monitored and logged. Please read the official US EPA warning below. The following activities are prohibited:

1. Obtaining, storing or distributing digital images over 5 Megabyte, any video files, music files, streaming media, such as RealMedia, QuickTime, and Windows Media; watching online videos/movies from inappropriate sites; watching Internet TV & listening to Internet radio; playing Internet games/group games, NetFlix, Hulu and other online streaming entertainment providers.
2. Streaming video from YouTube and other video rich sites to laptops, smartphones and tablets.
3. Storing, processing, displaying, transmitting prohibited content, i.e. adult content, sexually oriented material, nudity, militancy/extremist activities, terrorist activities, hate speech, or other activities that are illegal or inappropriate.
4. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.
5. Obtaining, installing copying, storing, or using software in violation of the appropriate vendor's license agreement.
6. Copying and posting controlled information, and/or personally identifiable information on commercial Internet sites.
7. Downloading and installing freeware/shareware or any other software product on the ship's laptops and/or servers.
8. Downloading/uploading files over 5 Megabytes.
9. Using copyrighted material in violation of the rights of the owner of the copyrights.
10. Using the Internet that would adversely reflect on the EPA or the R/V Lake Guardian such as chain letters, unofficial soliciting, selling, etc.
11. Using the Internet to conduct personal business.

##########-WARNING-###########

In proceeding and accessing U.S. Government information and information systems, you acknowledge that you fully understand and consent to all of the following:

1) you are accessing U.S. Government information and information systems that are provided for official U.S. Government purposes only;
2) unauthorized access to or unauthorized use of U.S. Government information or information systems is subject to criminal, civil, administrative, or other lawful action;
3) the term U.S. Government information system includes systems operated on behalf of the U.S.

Government;

4) you have no reasonable expectation of privacy regarding any communications or information used, transmitted, or stored on U.S. Government information systems;
5) at any time, the U.S. Government may for any lawful government purpose, without notice, monitor, intercept, search, and seize any authorized or unauthorized communication to or from U.S. Government information systems or information used or stored on U.S. Government information systems;
6) at any time, the U.S. Government may for any lawful government purpose, search and seize any authorized or unauthorized device, to include non-U.S. Government owned devices, that stores U.S. Government information;
7) any communications or information used, transmitted, or stored on U.S. Government information systems may be used or disclosed for any lawful government purpose, including but not limited to, administrative purposes, penetration testing, communication security monitoring, personnel misconduct measures, law enforcement, and counterintelligence inquiries; and
8) you may not process or store classified national security information on this computer system.

############-WARNING-############