Computers and Network Access

Email Access

While at CMEL, you can access your Lotus Notes mail using the computers located in the Library Resource Center (room C-235) or CoLab (room C-145). You are required to sign the access log in both facilities prior to using a computer. You should contact your facility's in-house computer support staff to obtain the URL or Web address to access your web-based Lotus Notes mail. Also confirm your web mail password, as it may not be the same as your Lotus Notes desktop client password.

CoLab Access

In the main training building's CoLab facility (room C-145), computers are available for guest use during times when staff or class use has not been specifically reserved. They are also available throughout after-class and overnight hours. Specific login and password information is posted beside each computer.

Personal Computers

Personal computers may be connected to the internet utilizing the wired high-speed public internet service in the guestrooms or the wireless public internet service. Connection in your guestroom is available using a standard network cable (RJ45 connectors), plugged into the wall receptacle found under the desk. We encourage you to bring this cable with you.

BE ADVISED: You should not connect your personal computer to the network outlets in the "C" building. The "C" building includes: classrooms, breakout rooms, and the CoLab (C-145).

Network Access

Only government-owned computers will be authorized to connect to the CMEL network. You **MUST** register your computer (laptop) at the Front Desk **prior** to accessing the INTERNET, INTRANET, or FTI system (FAA wide area network -- WAN).

If your computer is not DHCP configured (Dynamic Host Configuration Protocol), you will not be able to use the LAN connection. You may opt to contact your home technical support for assistance in configuring your computer.

Scanning software is in use at CMEL, Southern Region, and Headquarters. It scans all computers in the agency for viruses, software updates, hot fixes, and patches. If these are not installed on your laptop, the likelihood of infection is quite high. If this scan process shows your computer to be infected, you will be disconnected from the LAN.

CMEL also supports remote network access through the FAA Intranet using Winframe/Metaframe (Citrix) via a TCP/IP connection. Contact your administrator for any configuration information required to make this type of connection **prior to arrival** or **prior to attempting to make the connection**.

Computer Registration

Personal computers may be connected to the internet utilizing the high-speed public internet service in your assigned guestroom or the wireless public internet service. Only government-owed computers will be authorized to connect to the CMEL network. Prior to connecting to the CMEL network, you **MUST** register your computer (laptop) at the Front Desk.

Usage Rules

The practices below are designed to minimize security risks for CMEL and the computer user. All users will be held accountable for their actions associated with the access and intended use of the CMEL server and network, whether using their own government-issued computers or CMEL supplied computers.

Access to CMEL Trusted Network. The user is granted access to network for the purposes of conducting business with the FAA and all activities are to be beneficial for FAA.

Protection of Copyright Licenses (Software). Users shall not install unlicensed software on any device.

Authorized Use –FAA Internet resources shall be used:

a. For valid work requirements (e.g., exchange of information that supports the FAA mission, goals, and objectives; job-related professional development for FAA management and staff; access to scientific, technical, and other information that has relevance to FAA; and business-related communications with colleagues in government agencies, academia, and industry.

b. For limited personal use (e.g., brief communication or Internet searches), provided such use does not:
    1. Interfere directly or indirectly with FAA computer or networking services;
    2. Burden FAA with additional incremental costs;
    3. Interfere with an FAA user's employment or other obligations to the Government;
    4. Reflect negatively on the FAA or its employees; or
    5. Violate any Federal or FAA rules, regulations, or policies.

System Privileges. Users may have access to certain servers by virtue of their connection to the CMEL network. These servers are provided in trust that the user will not misuse the access or harm the FAA with this trust. Users are to work within the confines of the access allowed and are not to attempt access to systems or applications to which access has not been authorized.

Virus Protection. Users must have current anti-virus software enabled and active on their computer.

Security Patches. Users will certify that the operating system of their personal computer is patched with the latest security service packs or patches available and will be accountable to any security breaches encountered on their system.

Inappropriate Use of Access. Users will not activate on their desktop any type of Packet Capture application without prior approval. The user will not transmit packets for the purpose of assessing vulnerabilities of the network without prior approval. The user will not attempt to gain unauthorized access to any resources within FAA or any networks connected to FAA including the internet.

Permission of Inspection. The user will permit the inspection of their equipment connecting to the CMEL LAN for the purposes of compliance to these guidelines and as needed for resolution of any technical issue that may arise.