

Florida Museum of Natural History Network Access Policy

Introduction

The Office of Museum Technology (OMT) is responsible for maintaining the integrity of the Florida Museum of Natural History (FLMNH) network. The network includes the computer communication infrastructure as well as the network services such as email, the museum web site, museum databases, Internet connectivity, and various other services. The network is a shared resource that requires a certain level of trust between all connected devices. In order to maintain the availability and reliability of network resources for the museum, OMT has created this Network Access Policy. This Policy outlines the rules and requirements for network access at the museum. OMT will disconnect computers from the network that do not meet these requirements or are in violation of this network access policy. Computers that are found to pose a risk to the rest of the network will be disconnected.

If you become aware of people who are not adhering to the Network Access Policy, please report this to OMT so appropriate corrective action can be taken.

Network Access

Network users at the museum must comply with the University of Florida Office of Information Technology Acceptable Use Policy (AUP). As indicated in the AUP itself, this "applies to all users of university computing resources, whether affiliated with the university or not, and to all uses of those resources, whether on campus or from remote locations". The UF AUP is available online at <http://www.it.ufl.edu/policies/aupolicy.html>.

Network users at the museum must comply with the *FLMNH Software Copyright Policy*.

Computers will not function on the network until they have been registered with OMT.

OMT maintains records containing certain information about every networked device:

1. Network adapter Hardware Address, also known as Mac Address
2. Serial Number of the device
3. Physical location of the device (building, room number, etc.)
4. Owner or primary user of the device

This information is required for OMT to register the computer on the network. If the computer complies with the remainder of this *Network Access Policy*, OMT will assign an IP address and computer name.

Students and persons who do not work directly for the museum but would like access to the network or an email account must complete the *Florida Museum of Natural History Computer Systems Request Form (For Persons not appointed to FLMNH Payroll)*.

The Museum uses authentication and logging to identify users. Usernames and passwords are individually assigned and are not to be shared with others. Passwords are not to be shared with anyone, including supervisors. OMT can assist in setting up mechanisms for sharing files that do not require password sharing. When not actively using the computer, the system should be "locked" or the user should be "logged out" to prevent unauthorized users from sitting down at the computer and using the network. Please do not tape your password to your monitor, leave it under your keyboard, store it in an unlocked desk drawer, or leave it in a visible location.

Virus protection at the museum is a multi-tiered architecture. Virus protection is required on every Windows and Macintosh computer that connects to the museum network, including file servers, email servers, web servers, desktops, and laptops. McAfee VirusScan software is provided at no charge to each

individual through licensing agreements negotiated by the University of Florida. Please contact OMT to acquire this software.

Operating Systems and computer software often have security vulnerabilities. Patches and updates to known vulnerabilities must be applied before a computer will be permitted on the FLMNH network.

No devices will be connected to the network without previous authorization from OMT. This includes computers, servers, network printers, hubs, switches, routers, gateways, or any device that connects to the museum network cabling.

Wireless networking is available in some areas of FLMNH. Wireless networking is provided in accordance with wider UF wireless networking requirements. Always use the UF VPN Service when connecting over a wireless network. For more information, see the Wireless Networking Tutorial at <http://www.flmnh.ufl.edu/omt/wireless.htm>.

No unauthorized servers are permitted on the museum network. A server is software or hardware that allows remote access to resources. Web servers, FTP servers, music servers, etc. are not permitted without prior written permission from OMT. Generally speaking, Windows file and print sharing is permitted. Please contact OMT for assistance in setting up file sharing and to prevent unauthorized individuals from accessing your data files.

If OMT discovers a violation of this policy, appropriate action will be taken to remedy the situation. OMT will provide assistance to the individual. OMT may be required to disconnect network access if a risk has been discovered. The computer may be reconnected once the risk has been dealt with in a manner that is satisfactory to OMT.

Standards

Before purchasing new computer equipment or software, please contact OMT to make sure your purchase meets the current standards. OMT has no obligation to support newly acquired equipment if the equipment does not meet the current standards. Computers that do not meet the requirements will not be allowed to connect to the network. Please see the *Minimum Requirements for FLMNH Networked Computers* for more information.

Questions and Answers:

Q: My friend needs to type a paper. I let him into my office and give him my password so he can log in. Is this ok?

A: No. You have violated the museum network access policy by sharing your password.

Q: I have multiple grad students who share a computer. Is it ok to create a group account that they all can use?

A: No. Except in extreme circumstances, each individual user should have their own username and password.

Q: Why aren't I allowed to connect my Windows 98 computer to the network? My Windows 98 computer is perfectly fine.

A: Each networked device must meet certain requirements in order to be connected to the network. Windows 98 does not provide security and authentication. Additionally, it is much more susceptible to

attacks from across the network, is not supported by Microsoft anymore, and does not accept the standard McAfee VirusScan software reliably. Connecting a Windows 98 computer to the network puts all of the museum network services at risk.

Q: I just bought a brand-new computer that is running Windows XP Home Edition. Can I connect it to the network?

A: Only if you purchased the computer with your own funds. Persons using Windows XP Home Edition on their *privately owned* computer will be permitted to keep using it due to the lack of a major discount for individuals wishing to upgrade to the Pro Edition. (UF discounted licenses CANNOT be used for computers not owned by the University.) However, Windows XP Home Edition is designed for home use, not for business networks and individuals must be aware that this choice will limit their capabilities on the FLMNH network.

All university-owned Windows computers are expected to use a fully functional, network-capable operating system such as Windows 2000. Computers found to be running Windows 95/98 or XP Home Edition will be required to upgrade since UF departments receive a substantial cost savings on institutional licenses.