Desktop Computer Security Policy

Effective Date: 03/01/2009
Last Revised: 07/14/2015
Last Reviewed: 04/07/2017

Audience

Faculty, Staff

Policy

1. Definition

Desktop computers are personal workstations that, though possibly linked to other computers via a Local Area Network, function as stand-alone units. Desktop computers include PCs and Apples.

2. General Obligations

Users and administrators of shared Desktop computer stations are responsible for the oversight of these units and are subject to the Computer Use Policy and the IT Security Policy.

3. Hardware Security

1. Lock offices. Office keys should be registered and monitored to ensure they are returned when the employee leaves the Institute.
2. Secure Desktops in public areas. Equipment located in publicly accessible areas or rooms that cannot be locked should be fastened down by a cable lock system or enclosed in a lockable computer equipment unit or case.
3. Secure hard disks. External hard disks should be secured against access, tampering, or removal.
4. Client Technology Services department will maintain the physical inventory and proper identifying of all network computers.
5. Locate computers away from environmental hazards.
6. Critical data should be stored in those file locations that are backed up on a regular basis by Information Technology Services (network file share locations on mbistore or in the My Documents folder of your workstation).

4. Access Security

Utilize password facilities to ensure that only authorized users can access the system. All MBI computers will have password protected screen savers in place and the password protection will activate when the computer is inactive for 10 minutes.

Password guidelines:

- Length should be minimally six characters.
- Avoid words found in the dictionary and include at least one numeric character.
- Choose passwords not easily guessed by someone acquainted with the user. (For example, passwords should not be maiden names, or names of children, spouses, or pets.)
- Do not write passwords down anywhere.

- Change passwords every 180 days.

5. Data and Software Availability

- Check data and software integrity daily through Moody approved anti-virus software.
- Fix software problems immediately. If needed, contact the ITS Support Center for assistance.

6. Confidential Information

- Monitor printers used to produce sensitive and confidential information.
- Purge and securely sanitize sensitive files on all devices when their use is complete.
- Destroy any portable storage media that contain sensitive files when obsolete.

7. Software

Software is protected by copyright law. Unauthorized copying is a violation of the MBI Copyright policy. Anyone who uses software should understand and comply with the license requirements of the software. The Institute is subject to random license audits by software vendors.

8. Viruses

Computer viruses are self-propagating programs that infect other programs. Viruses and worms may destroy programs and data as well as using the computer's memory and processing power. Viruses, worms, and Trojan horses are of particular concern in networked and shared resource environments because the possible damage they can cause is greatly increased. Some of these cause damage by exploiting vulnerabilities in system software. Fixes to infected software should be made as soon as a problem is found.

To decrease the risk of viruses and limit their spread:

- Check all software before installing it.
- Use software tools to detect and remove viruses.
- Isolate immediately any contaminated system by disconnecting it from the network.
- Anti-virus software will be installed on all MBI owned machines.

9. Computer Networks

Networked computers may require more stringent security than stand-alone computers because they are access points to computer networks.

While Information Technology Services has responsibility for setting up and maintaining appropriate security procedures on the network, each individual is responsible for operating their own computer with ethical regard for others in the network environment.

The following considerations and procedures must be emphasized in a network environment:

- Check all files downloaded from the Internet. Avoid downloading shareware files.
- Test all software before it is installed to make sure it doesn't contain a virus/worm that could have serious consequences for other personal computers and servers on the MBI network.

- Use (where appropriate) a secure connection and authentication services to send confidential information over the MBI network.
- Never store MBI passwords or any other confidential data or information on your Moody laptop or personal PC or associated electronic media. All such information should be secured after any remote connection to the MBI network.

Definitions

n/a

Procedures

n/a

Documents

n/a

Contacts

If you have questions or concerns about the execution of this policy, you may contact the Information Technology Services Support Center at 312.329.4067 or ITS@moody.edu for assistance.

If you have questions about the policy, you may email ITSpolicy@moody.edu for assistance.

Related

- n/a