

McKnight Brain Institute

Policy: MBI-01	Category: Information Security	Version Date: August 30, 2006
Title: MBI Secure Computer Policy		Effective Date: September 1, 2006
Originating Unit: MBI	Last Review: September, 2006	
Review Resp: Frank Bova, PhD, ISA Joseph Schentrup, ISM	Next Review: August, 2007	

Purpose:

The purpose of this policy is to ensure computers installed in the McKnight Brain Institute (MBI) have identification information and meet the minimum SPICE standards for information security. The intention is to avoid disruption in computing service to other tenants at the MBI, as a result of network intruders, viruses, worms and other malicious or disruptive service that can affect many computers as a result of one unsecured computer.

Scope:

This policy applies to all networked computers residing in the MBI, regardless of ownership.

Reference(s):

1. UF HSC SPICE Policies and Standards

Policy:

1. Registration
 - a. All owners of computers to be networked in the MBI domain must register their computers and other network devices with the MBI CITS dept. Registration information must minimally included:
 - i. Contact information of user and system administrator (if different from user)
 - ii. Name of department
 - iii. Manufacturer and OS of computer
 - iv. Location and room
 - v. Machine name
 - vi. MAC Address
 - vii. IP address if static
 - b. All owners of computers to be networked in the MBI but not in the MBI domain must register their computers and other network devices with their HSC Unit ISM. Registration information must minimally included:
 - i. Contact information of user and system administrator (if different from user)

- ii. Name of department
 - iii. Manufacturer and OS of computer
 - iv. Location and room
 - v. Machine name
 - vi. MAC Address
 - vii. IP address if static
2. Antivirus protections:
 - a. All computers must have antivirus protection that is kept current.
 - b. The MBI CITS must be allowed to install antivirus compliance reporting software on networked computers in the MBI. CITS will make exceptions for computers already running antivirus compliance reporting software under another HSC Unit ISM's management.
 - c. Computers that cannot run antivirus software must be documented and isolated from harming other computers.
 - d. System administrators of computers that cannot run antivirus monitoring software must scan their computers with McAfee or other approved antivirus software and send a status report (antivirus activity log) of the currency and activity of their antivirus software, to MBI CITS once a week.
3. Software Patches:
 - a. All system administrators must monitor for security patches for software loaded on their computers and apply them.
 - b. Computer users and system administrators must permit the MBI CITS dept to monitor for outdated operating system patches.
 - c. Computers where OS patches for critical security vulnerabilities cannot be applied, must be isolated from harming other computers.
 - d. System administrators of computers where OS patches cannot be monitored must check the status of their OS vulnerabilities and send a report to MBI CITS once per month.
4. Computers installed at the MBI will be regularly scanned for malicious activity and vulnerabilities.
 - a. If known in the MBI computer registration database, system administrators of computers found vulnerable will be notified. Critical vulnerabilities must be resolved as soon as possible. If the system administrator of a vulnerable computer is not known, the vulnerable system may be disconnected from the network until identification is clear and the vulnerability is fixed.
 - b. Compromised computers will be disconnected from the network. If known in the MBI computer registration database, system administrators of computers found compromised will be notified prior to disconnecting. The computer must be rebuilt before it will be allowed back on the network.