II-175 Virus, Malicious Code and Unauthorized Code

Purpose

This policy ensures that software and information processing facilities are not vulnerable to malicious software, such as computer viruses, network worms, Trojan horse programs, “spam”, “adware”, and “spyware”. Users shall be made aware of the dangers of unauthorized or malicious software. Administrative and technical controls/software must be implemented and maintained to detect or prevent the introduction of such code. In particular, it is essential that precautions be taken to detect and prevent computer viruses and malicious software on personal computers.

Policy

Where technically capable, CCHMC Personnel must implement the following detection and prevention controls to protect against the introduction or propagation of mobile malicious code:

- Anti-virus detection procedures;
- Regular reviews of software and data content of systems;
- Checking untrusted or unauthorized file transfers;
- Checking electronic mail attachments;
- Virus attack response procedures;
- Vulnerability management and patch management procedures;
- Detecting and removing of spyware, adware or any other forms of malware; and
- Perform appropriate filtering and/or blocking of unsolicited email; also know as “spam”.

CCHMC must provide an education program to inform users of the varied threats that malicious and unauthorized code present, and of their responsibilities in preventing the introduction and propagation of such code.

Unauthorized Software

Installation of Unauthorized Software

The intentional installation of any software, utilities, helper objects, or any computer code not specifically approved for use on CCHMC computing systems is prohibited. Examples of unauthorized software include, but are not limited to:

- Peer-to-Peer file sharing applications such as Gnutella, Sharebear, LimeWire and Kazaa;
- ICQ or any Instant Messaging application not provided as part of the CCHMC standard software image;
- Remote control or access software such as GoToMyPC©, DameWare © or similar software;
- Any unauthorized software that automatically remembers login IDs/passwords such as Gator©, KeyRobot and Smart Login; and
- Entertainment Software such as WebShots, WeatherBug and Date Manager.

Removal of Unauthorized Software

- Unauthorized, malicious or nuisance software can be installed on a computer without the knowledge of the user. If unauthorized software is found or suspected of being on any CCHMC computer, the Information Services Service Desk should be contacted for assistance.
- Reporting unauthorized software is required so that the Department of Information Services can maintain a safe and reliable computing environment within CCHMC.
- Information Services may remove, with or without prior notification any malicious or unauthorized software.

Virus Protection

All CCHMC information assets must have functioning and up to date anti-virus software installed, as technically available. The requirements of policy include but are not limited to all computing devices that electronically connect to the CCHMC network including non-CCHMC owned computers, wireless connections, personal computers, vendors and consultants. Compliance with this policy must be verified by Information Services or designated representative prior to any connection to the CCHMC network. For non-CCHMC owned computing devices antivirus applications must be approved by Information Services.

Anti-virus signatures/definition sets must be updated as soon as practically possible.

Where technically supported, all information assets will participate in the CCHMC automated antivirus management system. Where this cannot be achieved, alternate risk mitigation methods must be implemented (e.g. network-based intrusion prevention/detection). Remote access users and non-CCHMC computing devices must employ reasonable and appropriate antivirus capabilities, and are not required to participate in the automated antivirus management system.

Where information assets cannot participate in the CCHMC antivirus management system, documented justification must be submitted to the Director of Information Security for approval and determination of alternate methods of risk mitigation.

Users may not disable this software or the updates, without written permission from the Director of Information Security, or the Chief Information Services Officer.

The deliberate creation, use, storage, distribution and/or possession of malicious mobile code is expressly prohibited.

The intentional storage, distribution and/or possession of malicious mobile code may be construed as failure to safeguard CCHMC computer resources.

Reporting

Users who believe that CCHMC computer resources (including workstations) under their control have been compromised by mobile malicious code shall immediately notify the Information Services Service Desk (x64100) for further guidance.

Users shall not disseminate hoax messages received via email. Users who receive virus-related warnings from other than Information Services shall contact the Information Services Service Desk for further clarification and/or guidance.

All virus, worm or Trojan activity must be reported to the Information Services Service Desk.

E-mail Antivirus Best-Practice

Users shall take due care when opening suspicious or unexpected email with attachments from unknown users outside of CCHMC. When in doubt contact the Information Services Service Desk. Refer to the email Guideline.

Hoax Messages

Forwarding of hoax messages is expressly prohibited.

When uncertain, users shall contact the Information Services Service Desk for assistance and/or guidance.

Hoax messages spread fear and uncertainty, and cause loss of productive time by users and Information Services staff. Hoax messages are usually passed on to other users out of ignorance, rather than malice.

These messages often:

- Report a threat of a virus that can do massive damage to your pc - many even going so far as to say that critical hardware will be destroyed.
- Sound unnecessarily technical (although often meaningless), thus taking advantage of many users fears of technology/the unknown.
- May quote bogus announcements from antivirus industry experts, some even going so far as to provide a correct link to an antivirus vendor site.
- May be written in emotive language – lots of upper case letters and exclamation points in order to emphasize the “severity” of the message, and make the user more likely to forward the message to others.
- May ask you to forward the message to as many people as possible; this is often the most obvious giveaway.
- The “remedies” contained in these warnings are often destructive in nature themselves, and may render a workstation inoperable.
- Ironically, hoax messages can mimic virus-like symptoms. In addition to causing undue concern, widespread forwarding of hoax messages may congest e-mail systems and utilize extensive quantities of disk space on e-mail servers.

Spyware Protection

“Spyware” is any software that gathers specific user information without the user’s knowledge, and then relays this information, via the Internet, to unauthorized interested parties who may use this information for profiling or targeting attempts. Appropriate security controls shall be implemented to detect and remove spyware on CCHMC systems and computers, where technically capable.

Alerts, Advisories, and Notices

Awareness of information technology security alerts, advisories, and notices are necessary to maintain the effectiveness and integrity of CCHMC’s information technology security architecture. As vulnerabilities are identified in systems, and security fixes are distributed, all applicable remediation steps shall be implemented in a timely manner to mitigate potential information technology security threats.

Applicability

This policy applies to all CCHMC Personnel and any other party who is authorized to access the CCHMC network including Medical Staff members, remote access users, consultants, temporary employees, and vendors.

Regulatory Authority

HIPAA Regulations: 45 CFR Subtitle A, Subchapter C, Part 164

164.308 Administrative safeguards.

- ➢ (a)(5)(ii)(B) Implementation specifications: Protection from malicious software.
- ➢ (a)(6)(ii) Implementation specifications: Response and reporting.

Compliance

All CCHMC Personnel, community physicians, and business partners must comply with this policy and the associated standards and procedures. Any CCHMC Personnel found to be in violation of the privilege of CCHMC-facilitated access to business systems, or in violation with this policy, may be subject to disciplinary action, up to and including termination of employment. Medical Staff Members may also be subject to denial or removal of their privileges as part of the disciplinary process. Federal, state, and/or local law enforcement agencies may be notified if evidence of criminal actions exists. Any business partner found to be in violation of the privilege of CCHMC-facilitated access to business systems, or in violation with this policy, may be sanctioned, which could include, denial of access to the CCHMC network, cancellation of any contractual agreement between CCHMC and the business partner, discipline by the Medical Staff, and any other action deemed appropriate.

Refer to CCHMC Personnel Policy F-05 Employee Discipline for additional information regarding disciplinary action.

Implementation

The following parties are responsible for implementing and enforcing this policy:

- Policy authority for this document resides with the Chief Information Services Officer and the HIPAA Security Officer.
- All requests for exceptions to this policy or its standards must be submitted in writing, with justification to the HIPAA Security Officer (securityofficer@cchmc.org).

This policy has been reviewed and approved by the following parties:

- Chief Executive Officer
- Chief Information Services Officer
- HIPAA Security Officer

This policy will be reviewed every 3 years or sooner if deemed necessary.