UNC-CH School of Dentistry Policy
Malware/Reimaging

Introduction
One of the most prevalent challenges to IT Services is Personal Computer (PC) virus/spyware/malware infection. Such infections can destroy data or file systems or render a computer inoperative. The potential to damage the School of Dentistry’s (SoD’s) information network grows the longer an infected PC is connected to the network.

Purpose of Policy
To confirm and amplify the School of Dentistry’s adherence to University Information Technology Service Policies regarding protection of SoD’s information networks.

Audience
This Policy applies to all SoD Faculty, Staff, Administrators and Students utilizing Windows or Macintosh Personal Computers for School activities.

Definitions
Malware – Malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, trojan horses, and spyware.

- **Virus** – Computer viruses are small programs or scripts that can negatively affect the health of your computer.1
  - **Browser Virus** – A browser hijacker (sometimes called hijackware) is a type of malware program that alters your computer’s browser settings so that you are redirected to Web sites that you had no intention of visiting.
  - **Worm(s)** – A computer worm is a type of virus that replicates itself, but does not alter any files on your machine. However, worms can still cause havoc by multiplying so many times that they take up all your computer’s available memory or hard disk space.
- **Trojan Horse(s)** – Trojan horses are software programs that masquerade as regular programs, such as games, disk utilities, and even antivirus programs. But if they are run, these programs can do malicious things to your computer.
- **Spyware** – Spyware can capture information like Web browsing habits, e-mail messages, usernames and passwords, and credit card information. If left unchecked, the software can transmit this data to another person’s computer over the Internet.

---

1 Some viruses can duplicate themselves, attach themselves to programs, and travel across networks. In fact opening an infected e-mail attachment is the most common way to get a virus.
UNC-CH School of Dentistry Policy
Malware/Reimaging

**Reimage** – Reimage is the process of wiping a computer hard drive(s) and reinstalling the operating system and standard software. A reimage is necessary if the operating system becomes damaged, corrupted or the system is plagued with malware problems.

**Policy**

**Policy Statement**
All University-owned Computers (desktop and laptop) shall have University approved anti-virus software installed.

If the device stores or processes sensitive information, OCIS staff is required to contact the University Information Security Office and report the malware as a critical security incident as required in the University Incident Management Procedures. The UNC Information Security Office will then determine how best to proceed for the purposes of preserving evidence and ensuring an audit trail for the investigation of the incident.

All University-owned Computers used by SoD Faculty, Staff, Administrators and Students are subject to possible reimaging if found to be infected with malicious software. **In the event of reimaging, all data contained on the computer may be lost.**

**Compliance**

**Compliance Statement**
The potential risk for destruction of SoD Institutional, Business and Research data due to malicious software rises with every infected Personal Computer that connects to the SoD network. This document is created to shrink those risks by establishing positive controls ensuring each User complies with University Policies.

**Roles and Responsibilities**

**OCIS** –

1. Shall create and reserve space on the Storage Area Network (SAN) for use by all Users to store personal data.
2. Shall create, distribute and maintain processes and procedures governing protection from and/or response to malicious software infection of SoD servers and network components.
3. Shall create, **distribute and maintain processes and procedures governing response to malicious software infection** of Personal Computers.

**Individual Users** –

---

2 In this context either desktop or laptop

Approved 12/16/2016
UNC-CH School of Dentistry Policy
Malware/Reimaging

1. Are responsible for knowing and following the OCIS Best Practices
2. Are responsible for re-loading any data lost due to reimaging.
3. Shall immediately disconnect the Personal Computer from the SoD network and notify OCIS when infection is suspected.

Procedures to comply with policy

1. The University’s Information Technology Systems (ITS) department offers the following anti-virus/malware tools:
   - Microsoft Windows – Includes Windows Defender antivirus. University-owned computers will have Microsoft System Center Endpoint Protection installed.
   - Apple Macintosh – Microsoft System Center Endpoint Protection
2. The University offers several methods of data backup. Refer to the ITS Help and Support Data Backup Web Page for more information.
3. OCIS provides support for School-owned and personally owned computers as defined by OCIS Policy
4. OCIS personnel shall make reasonable, best efforts to remove the malware; however if efforts fail, the computer hard disk will be reimaged. In the event of reimaging, all data contained on the computer may be lost.

Related Data

Appendices
OCIS Active Malware Policy dated August 11, 2012

Contacts

Questions
David B. Rankin, IT Director SoD, Security Liaison SoD 919-537-3485

Violations
David B. Rankin, IT Director SoD, Security Liaison SoD 919-537-3485

Consulting
OCIS Staff, 919-537-3485
UNC Help Desk, 919-962-4357
UNC Information Security Office, 919-445-9393

History

<table>
<thead>
<tr>
<th>Version</th>
<th>Effective Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>04/23/2015</td>
<td>TAD</td>
</tr>
<tr>
<td>2</td>
<td>12/16/16</td>
<td>GDM</td>
</tr>
</tbody>
</table>

Approved 12/16/2016
UNC-CH School of Dentistry Policy
Malware/Reimaging

Next Review Date: 12/16/2017

Authorization

Kenneth May, Dean, UNC School of Dentistry

Signature _____________________________________________

Date ________________________________________________
Office of Computing and Information Systems

Active Malware Policy

Email message sent to SOD community on August 11, 2012

If malware is reported in a computer support ticket or is discovered as part of a routine computer support call, I am requiring OCIS support staff to interactively determine if a device processes or stores sensitive information as defined by the University Information Security Policy. If the device does store or process sensitive information, OCIS staff will be required to contact the University Information Security Office and report the malware as a critical security incident as required in the University Incident Management Policy, pages 4-5. The UNC Information Security Office will then determine how best to proceed for the purposes of preserving evidence and ensuring an audit trail for the investigation of the incident.

I apologize in advance for any inconvenience this may cause. To avoid your computer being infected by malware, please follow these best practices:

1. Make sure your computer's firewall, anti-virus and anti-spyware programs are running and are up-to-date. If you are not certain, please contact OCIS.
2. Make sure your computer is receiving and applying the latest operating system and application patches. If you are not certain, please contact OCIS.
3. Avoid downloading and installing programs. If you must, then only download programs from websites you trust. If you're not sure whether to trust a program you are considering downloading, enter the name of the program into your favorite search engine to see if anyone else has reported that it contains spyware.
4. Carefully read all security warnings, license agreements and privacy statements associated with any software you download.
5. Never click "Agree" or "OK" to close a window. Instead, click the red "x" in the corner of the window or press Alt + F4 on your keyboard to close a window.
6. Beware of free programs and be sure you understand all of the software packaged with those programs.
UNC-CH School of Dentistry Policy
Malware/Reimaging

7. Use a standard user account instead of an administrator account in your day-to-day computer use. For more information about this, contact OCIS to see if you can use a standard user account on your computer.