UNC-CH School of Dentistry Policy
Non-Secure Servers

Introduction
Non-Secure servers, desktop computers with server software installed and operating as a server, represent a threat vector to the security of SoD information. Legal, logistic and financial forces strongly influence the need to enforce standards on such computers.

A server is a computer designed to process requests and deliver data to other (client) computers over a local network or the Internet. This includes, but is not limited to, file shares, printer sharing, Web page, File Transfer Protocol (FTP), etc.

Purpose of Policy
To establish scope and standards for individual non-secure servers operating on the SoD networks.

Audience
The Policy applies to all SoD Faculty, Staff, Students, Visitors and Temporary Employees utilizing the SoD networks.

Definitions
Computer – An electronic device for storing and processing data according to instructions given to it in a variable program. A computer can be a desktop or portable laptop machine with at least one processing element, typically a central processing unit (CPU), some form of memory and internal hard disk storage.

Non-Secure Server – Any server-configured computer not managed or administered by OCIS, is connected to the SoD network and does not contain and does not have access to SoD Secure Data.

OCIS – SoD Office of Computing and Information Systems

Patch – A piece of software designed to update a computer program or its supporting data, to fix or improve it. A security patch is a change applied to an asset to correct the weakness described by a vulnerability. This corrective action will prevent successful exploitation and remove or mitigate a threat’s capability to exploit a specific vulnerability in an asset.

---

1 While server software is specific to the type of server, the hardware is not as important. In fact, regular desktop computers can be turned into a server by adding the appropriate software.
2 Refer to UNC-CH School of Dentistry Secure Data Policy for more detail

Approved on: 12/16/2016
UNC-CH School of Dentistry Policy
Non-Secure Servers

Policy

Policy Statement
1. All Personal Computers configured for or operating as a server shall be registered with and approved by OCIS prior to operation. All such computers shall be subject to periodic security screening.
2. No independently administered server may have access to or store any SoD Secure Data at any time.
3. All independently administered Non-Secure Servers shall have root/administrator accounts restricted and secured with strong passwords.
4. No server administration support is provided by OCIS.

Compliance

Compliance Statement
Independently managed servers are threat vectors to the security of the School of Dentistry’s secure information. No unregistered server may be operated on SoD networks at any time.

Roles and Responsibilities
1. Individuals operating an approved server-configured computer are responsible for:
   a. Proper administration, security and data content
   b. Any security breach traceable to the individual’s server
   c. Prompt registration of any server they intend to connect to the SoD network
   d. Prompt update of all security patches
2. OCIS is responsible for administration and enforcement of this Policy

Procedures to comply with policy
1. Individuals responsible for the operation and administration of a server shall:
   a. Register the server with OCIS
   b. Ensure all applicable versions of available operating system patches are installed and remain current
   c. Ensure all application software patches are installed and remain current
   d. Ensure no SoD Secure Data is stored on the server
2. OCIS shall:
   a. Create and maintain Departmental processes and procedures to administer this Policy
Related Data

Policies
1. University of North Carolina Information Security Policy
2. University of North Carolina Transmission of Protected Health Information and Personal Identifying Information Policy
3. UNC-CH School of Dentistry Incident Management Plan
4. UNC-CH School of Dentistry Secure Data Policy
5. UNC-CH School of Dentistry Encryption Policy
6. UNC-CH School of Dentistry Application Inventory, Support and Registration Policy

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>12/16/2016</td>
<td>GDM</td>
</tr>
</tbody>
</table>

Next Review Date 12/16/2017

Authorization

Kenneth May, Dean, UNC School of Dentistry

Signature ________________________________

Date ________________________________

Approved on: 12/16/2016