PCI Windows Configuration Standard

Policy Title:
PCI Windows Configuration Standard

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Officer

Contact(s):
If you have questions about this standard, please contact the University Information Security Office.

I. Policy Statement

Microsoft Windows Servers within a high security environment. To adhere to standards for deploying Windows Servers to ensure security standards within the high security environment are upheld.

II. Definitions

Not applicable.

III. Policy

1. When setting up a Windows Server, select and configure the following options:
    a. Active Windows: Insert the appropriate MS Windows License key
    b. Set Time Zone: UTC-06:00) CST (US and Canada)
    c. Provide Computer Name and Domain: Change ONLY the COMPUTER NAME at this point. It will ask for a reboot. do NOT reboot yet
2. Use the Windows Start button, locate Network and "right-click"
    a. Select Properties then Change Adapter Settings
    b. Right-click the adapter and check only:
        i. Client for MS Networks
        ii. QoS Packet Scheduler
        iii. File and Print Sharing
        iv. IPv4
    c. Configure TCP IP setting for the IPv4 option assigning the IP address this server will use, along with the default gateway, DNS and WINS then save
3. Go back into the server console and reboot

4. Select "Download and Install Updates". Select all applicable MS updates for this server
5. Reboot if needed (repeat steps until no more updates are available)
6. Login with local administrator account
7. Add the server to Active directory using the appropriate AD credentials
8. Reboot
9. Login with the local administrator account
    a. Verify "Domain Admins" are in the local Administrators group, if not, add it.
    b. Verify ITS_SMA is added to the local Administrators group, if not, add it.
    c. Verify the firewall is ON. (this should already be turned on)
    d. Disables any rules on the firewall related to IPv6
    e. Use "nmap" SYN method to scan the server for open ports between 1-65535
    f. Reconfigure firewall if needed to restrict open ports. Only permitted TCP ports for a standard server should be:
        i. 135 RPC
        ii. 139 SMB
        iii. 445 MSDS
        iv. 3389 RDP
        v. 12489 NS+Client
        vi. 49154 DFS Management
10. Verify that TSM, NSClient+, and SNARE are all installed

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Standard at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- Security Policy

Approval Authority:	ITESC	**Approval Date:**	August 19th, 2014
Review Authority:	Jim Pardonek	**Review Date:**	July 7th, 2024

Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu