Secure Server Configuration Checklist

Ownership and Inventory

Server Local Hostname _____

- Must conform to OIT's server naming standard (see **Appendix A**)

Server DNS Hostname(s):_____

In the event of issues with this server, who should be contacted? _____

What Services does the server provide?_____

_____

Describe the data to be stored on the server by its categorization per our Data Stewardship Policy:

Public Data: _____

Protected Data: _____

Restricted Data: _____

Below is the list of specific settings and configurations required of all CMU servers:

Check each item in the following sections that have been verified to be true.

Basic Controls

☐ The server is protected with a host-based firewall.

☐ The server is protected with a network firewall at the edge of its network.

☐ Inbound firewall rules are whitelist-based.

☐ All firewall rules have a defined scope.

☐ The OS installed on the server has been installed by the OIT Systems Team, or installed with an approved image provided by the OIT Systems Team using the approved build checklists which can be found at:
https://cmich.teamdynamix.com/TDClient/KB/ArticleDet?ID=35905 for Windows and
https://cmich.teamdynamix.com/TDClient/KB/ArticleDet?ID=35906 for Linux

☐ Only software necessary for the server's primary function has been installed and enabled on the server.

☐ Additional software components added above and beyond the base OS install are documented with the OIT Systems Team.

☐ Superfluous services provided with the base OS install have been removed or disabled.

☐ The server uses the appropriate NTP servers. In most cases, these are the domain controllers.

☐ OS and software patching is set to be performed in accordance to OIT's standard patching practices or according to the vendor's patch release schedule. See **Appendix A** for the patching schedule.

☐ Server data is properly backed up to another system following OIT's backup policy. See **Appendix A**.

☐ Where possible, access controls to file, data, and applications follow a role-based model.

☐ Unnecessary user accounts have been removed from the system.

☐ Elevated privileges are restricted to "IT-" accounts. Tools such as sudo, runas, or UAC may be used to temporarily elevate privileges of user accounts.

☐ Where possible, administrative accounts are linked to specific individuals.

☐ Shared administrator accounts, where absolutely necessary, have their passwords and use restricted and protected to the fullest extent possible.

☐ Passwords adhere to the same complexity rules as stated in CMU's Global ID Password Policy.

☐ Default passwords for built-in accounts have been changed and adhere to the same complexity rules as stated in CMU's Global ID Password Policy.

☐ Automatic idle log-off of administrative user sessions must be set to the minimum time necessary to properly administer the server or service.

☐ Remote Administration access is secured with appropriate network encryption protocols.

☐ Direct server logon capability has been disabled for accounts that do not require it.

☐ User accounts of persons unaffiliated with CMU (such as hired contractors and consultants) are limited to a specific period of time required for the purposes of their engagement or support

assistance. These accounts provide only the necessary minimum level of access that is required for the task for which they have been contracted.

☐ The latest firmware has been applied for applicable components.

☐ IPv6 should be disabled where possible.

Server Security Monitoring and Protection

☐ Server is running Intrusion Detection and Prevention software approved by the Information Security Office. See **Appendix A** for approved list.

☐ Logs are collected and monitored for security-related events.

☐ All servers will be monitored by OIT Systems monitoring solution(s). See **Appendix A** for approved list.

☐ Logs are replicated on a system other than the server generating the logs, or to the Information Security Office's SIEM.

☐ The server will be scanned for vulnerabilities on a monthly basis and addressed in accordance to OIT's vulnerability management standard practice. See **Appendix A**.

☐ OIT's Systems Team has been granted and will maintain administrative access at all times by adding the appropriate AD group to the local administrator group and/or installing the OIT Systems Team's public SSH key.

☐ The appropriate vendor management tools and drivers have been installed, such as HP Service Pack for ProLiant for HP servers.

Additional Controls for Restricted Data

☐ OIT's advanced auditing software is installed.

☐ Backups are encrypted at rest.

☐ Server is set to be placed on the appropriate VLAN (PCI, HIPAA, etc)

Servers that contain Restricted Data need to meet the criteria listed in each section above, as well as any specific controls necessary to meet regulatory requirements.

Appendix A

OIT's Server Naming Standard

Server name shall begin with the prefix for the college or department the server is managed by, followed by a dash (-) (e.g. it-, cba-, se-, etc.). The server name shall not be more than 15 characters total. The server name will only contain alphanumeric characters and dashes (-).

OIT's Standard Patching Practices

Servers will fall in one of three categories: Test, Production, Production Critical. Test servers apply all available patches the Wednesday after they are released. Production will follow one week after test. Production Critical will follow two weeks after test. If a tiering solution is not available, patches will be applied the Wednesday after they become available.

OIT's Server Backup Policy

By default, all servers will be backed up to a secondary location with a minimum 10-day retention.

Intrusion Detection and Prevention software

The following are approved by the Information Security Office:

Windows OS:

- Windows Defender
- Wazuh HIDS

Linux OS:

- clamav
- Wazuh HIDS

OIT's vulnerability management standard practice

All servers will be scanned for vulnerabilities the first Friday of every month. The vulnerability scanner must have credentials to access every server and the ports for the credential scan (see below) must be set to allow access from the scanner's IP.

Scanner IP: 141.209.15.119

Windows Firewall Requirements:

- Windows Management Instrumentation (Async-In)
- Windows Management Instrumentation (WMI-In)
- Windows Management Instrumentation (DCOM-In)

Linux Firewall Requirements:

- SSH Port 22