NNT SECURITY THROUGH SYSTEM INTEGRITY NOW PART OF netwrix

NNT HIPAA Microsoft Windows 10 Enterprise 1709 Benchmark

18/10/2018 14:16

WIN-5L54AHGADT2 (192.168.17.18)

Compliance Score : 35.34%

246 of 696 rules passed
0 of 696 rules partially passed
450 of 696 rules failed

4.1. Security Management Process (§ 164.308(a)(1))

1. HIPAA Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations.

Identify Relevant Information Systems (Network Inventory Scan), Conduct Risk Assessment (Assess Configuration Vulnerabilities), Implement a Risk Management Pr

Rule Name	Score	Pass / Fail
Identify all information systems that house EPHI, including all hardware and software that are used to collect, store, process, or transmit EPHI, Implement security me	1	Pass

4.2 Assigned Security Responsibility (§ 164.308(a)(2))

HIPAA Standard: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for th

Identify the individual who has final responsibility for security, document the assignment to one individual's responsibilities in a job description

Rule Name	Score	Pass / Fail
Who in the organization is authorized to accept risk from information systems on behalf of the organization?	1	Pass

4.3 Workforce Security (§ 164.308(a)(3))

HIPAA Standard: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information

1-3 Implement Procedures for Authorization and/or Supervision, Establish Clear Job Descriptions and Responsibilities, Establish Criteria and Procedures for Hiring, W

Rule Name	Score	Pass / Fail
Implement Procedures for Authorization and/or Supervision	1	Pass

4.4 Information Access Management (§ 164.308(a)(4))

HIPAA Standard: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirem

Isolate Healthcare Clearinghouse Functions, Implement Policies and Procedures for Authorizing Access, Implement Policies and Procedures for Access Establishmen

Rule Name	Score	Pass / Fail
Determine if a component of the covered entity constitutes a healthcare clearinghouse under the HIPAA Security Rule,	1	Pass

4.5 Security Awareness and Training (§ 164.308(a)(5))

HIPAA Standard: Implement a security awareness and training program for all members of its workforce (including management)

Conduct a Training Needs Assessment, Develop and Approve a Training Strategy and a Plan, Develop Appropriate Awareness and Training Content, Materials, and M

Rule Name	Score	Pass / Fail
Implement a security awareness and training program for all members of its workforce (including management)	1	Pass

4.6. Security Incident Procedures (§ 164.308(a)(6)))

HIPAA Standard: Implement policies and procedures to address security incidents.

Determine Goals of Incident Response, Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism, Develop and

Rule Name	Score	Pass / Fail
Implement policies and procedures to address security incidents.	1	Pass

4.7. Contingency Plan (§ 164.308(a)(7))

HIPAA Standard: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, sy

Develop Contingency Planning Policy, conduct an Applications and Data Criticality Analysis, Identify Preventive Measures

Rule Name	Score	Pass / Fail

Establish policies and procedures for responding to an emergency or other occurrence.	1	Pass

4.8. Evaluation (§ 164.308(a)(8))

HIPAA Standard: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in respo

Determine Whether Internal or External Evaluation Is Most Appropriate, Develop Standards and Measurements for Reviewing All Standards and Implementation Spec

Rule Name	Score	Pass / Fail
Perform a periodic technical and nontechnical evaluation.	1	Pass

4.9. Business Associate Contracts and Other Arrangements (§ 164.308(b)(1))

HIPAA Standard: A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected healt

Identify Entities that Are Business Associates under the HIPAA Security Rule, Establish Process for Measuring Contract Performance and Terminating the Contract if

Rule Name	Score	Pass / Fail
The covered entity must obtain, document and measure performance of satisfactory assurances that the business associate will appropriately safeguard the EPHI inf	1	Pass

4.10. Facility Access Controls (§ 164.310(a)(1))

HIPAA Standard: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed,

Conduct an Analysis of Existing Physical Security Vulnerabilities and Identify Corrective Measures. Develop a Facility Security Plan, Access Control and Validation Pr

Rule Name	Score	Pass / Fail
Inventory facilities and identify shortfalls and/or vulnerabilities in current physical security capabilities, correct deficiencies and ensure that proper access is allowed. In	1	Pass

4.11. Workstation Use (§ 164.310(b))

HIPAA Standard: General System Hardening - Implement policies and procedures that specify the proper functions to be performed, the manner in which those functi

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: System Hardening - De

Rule Name	Score	Pass / Fail
Ensure 'Accounts: Guest account status' is set to 'Disabled'	1	Pass
Configure 'Accounts: Rename administrator account'	0	Fail
Configure 'Accounts: Rename guest account'	0	Fail
Ensure 'Enable screen saver' is set to 'Enabled'	0	Fail
Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr'	0	Fail
Ensure 'Password protect the screen saver' is set to 'Enabled'	0	Fail
Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'	0	Fail
Ensure 'Turn off Help Experience Improvement Program' is set to 'Enabled'	0	Fail
Ensure 'Allow Use of Camera' is set to 'Disabled'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: System Hardening - At

Rule Name	Score	Pass / Fail
Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: System Hardening: Gro

Rule Name	Score	Pass / Fail
Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	0	Fail
Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'	0	Fail
Ensure 'Continue experiences on this device' is set to 'Disabled'	0	Fail
Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'	1	Pass

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Internet Communicatio

Rule Name	Score	Pass / Fail
Ensure 'Turn off access to the Store' is set to 'Enabled'	0	Fail
Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'	0	Fail
Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled'	0	Fail
Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled'	0	Fail
Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled'	0	Fail
Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'	0	Fail

Ensure 'Turn off printing over HTTP' is set to 'Enabled'	0	Fail
Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (CCE Reference : CCE-33216-3)	0	Fail
Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'	0	Fail
Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled'	0	Fail
Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled'	0	Fail
Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled'	0	Fail
Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'	0	Fail
Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Personalization Rules

Rule Name	Score	Pass / Fail
Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (CCE Reference : CCE-35799-6)	0	Fail
Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (CCE Reference : CCE-35800-2)	0	Fail
Ensure 'Allow Input Personalization' is set to 'Disabled'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Search Rules

Rule Name	Score	Pass / Fail
Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	0	Fail
Ensure 'Allow Cortana' is set to 'Disabled'	0	Fail
Ensure 'Allow Cortana above lock screen' is set to 'Disabled'	0	Fail
Ensure 'Allow search and Cortana to use location' is set to 'Disabled'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Windows Installer Rules

Rule Name	Score	Pass / Fail
Ensure 'Allow user control over installs' is set to 'Disabled'	0	Fail
Ensure 'Always install with elevated privileges' is set to 'Disabled'	0	Fail
Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled'	0	Fail
Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled'	0	Fail
Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'	0	Fail
Ensure 'Allow Remote Shell Access' is set to 'Disabled'	0	Fail
Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'	0	Fail
Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'	0	Fail
Ensure 'Always install with elevated privileges' is set to 'Disabled'	0	Fail
Ensure 'Prevent Codec Download' is set to 'Enabled'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Administrative Templat		
Rule Name	**Score**	**Pass / Fail**
Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver'	0	Fail
Ensure 'Configure SMB v1 server' is set to 'Disabled'	0	Fail
Ensure 'Enable Structured Exception Handling Overwrite Protection (SEHOP)' is set to 'Enabled'	1	Pass
Ensure 'Turn on Windows Defender protection against Potentially Unwanted Applications' is set to 'Enabled'	0	Fail
Ensure 'Allow Windows to automatically connect to suggested open hotspots, to networks shared by contacts, and to hotspots offering paid services' is set to 'Disable	0	Fail
Ensure 'Remote host allows delegation of non-exportable credentials' is set to 'Enabled'	0	Fail
Ensure 'Configure Authenticated Proxy usage for the Connected User Experience and Telemetry service' is set to 'Enabled: Disable Authenticated Proxy usage'	0	Fail
Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled'	0	Fail
Ensure 'WDigest Authentication' is set to 'Disabled'	0	Fail
Ensure LAPS AdmPwd GPO Extension / CSE is installed	0	Fail
Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled'	0	Fail
Ensure 'Enable Local Admin Password Management' is set to 'Enabled'	0	Fail
Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters'	0	Fail
Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more'	0	Fail
Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer'	0	Fail
Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'	0	Fail
Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)')	0	Fail
Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'	0	Fail
Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'	0	Fail
Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled'	0	Fail
Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled'	0	Fail
Ensure 'Include command line in process creation events' is set to 'Disabled'	0	Fail
Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled'	0	Fail
Ensure 'Block user from showing account details on sign-in' is set to 'Enabled'	0	Fail
Ensure 'Untrusted Font Blocking' is set to 'Enabled: Block untrusted fonts and log events'	0	Fail
Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	0	Fail
Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'	0	Fail
Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'	0	Fail
Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled'	0	Fail
Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled'	0	Fail
Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled'	0	Fail
Ensure 'Turn off the advertising ID' is set to 'Enabled'	0	Fail
General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Administrative Templat		
Rule Name	**Score**	**Pass / Fail**
Ensure 'Enable Windows NTP Client' is set to 'Enabled'	0	Fail
Ensure 'Enable Windows NTP Server' is set to 'Disabled'	0	Fail
Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled'	0	Fail
Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'	0	Fail
Ensure 'Require pin for pairing' is set to 'Enabled'	0	Fail
Ensure 'Do not display the password reveal button' is set to 'Enabled'	0	Fail
Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled'	0	Fail
Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]'	0	Fail
Ensure 'Disable pre-release features or settings' is set to 'Disabled'	0	Fail
Ensure 'Download Mode' is NOT set to 'Enabled: Internet'	0	Fail
General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Administrative Templat		
Rule Name	**Score**	**Pass / Fail**
Ensure 'Do not show feedback notifications' is set to 'Enabled'	0	Fail
Ensure 'Toggle user control over Insider builds' is set to 'Disabled'	0	Fail
Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled: Warn'	0	Fail

Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'	0	Fail
Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	0	Fail
Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'	0	Fail
Ensure 'Turn off Windows Location Provider' is set to 'Enabled' (CCE Reference : CCE-33743-6)	0	Fail
Ensure 'Block all consumer Microsoft account user authentication' is set to 'Enabled'	0	Fail
Ensure 'Allow Address bar drop-down list suggestions' is set to 'Disabled'	0	Fail
Ensure 'Allow Adobe Flash' is set to 'Disabled'	0	Fail
Ensure 'Configure the Adobe Flash Click-to-Run setting' is set to 'Enabled'	0	Fail
Ensure 'Allow Extensions' is set to 'Disabled'	0	Fail
Ensure 'Do not use diagnostic data for tailored experiences' is set to 'Enabled'	0	Fail
Ensure 'Allow InPrivate Browsing' is set to 'Disabled'	0	Fail
Ensure 'Configure cookies' is set to 'Enabled: Block only 3rd-party cookies' or higher	0	Fail
Ensure 'Configure Password Manager' is set to 'Disabled'	0	Fail
Ensure 'Configure Pop-up Blocker' is set to 'Enabled'	0	Fail
Ensure 'Configure search suggestions in Address bar' is set to 'Disabled'	0	Fail
Ensure 'Configure Windows Defender SmartScreen' is set to 'Enabled'	0	Fail
Ensure 'Enables or disables Windows Game Recording and Broadcasting' is set to 'Disabled'	0	Fail
Ensure 'Prevent access to the about:flags page in Microsoft Edge' is set to 'Enabled'	0	Fail
Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for files' is set to 'Enabled'	0	Fail
Ensure 'Prevent bypassing Windows Defender SmartScreen prompts for sites' is set to 'Enabled'	0	Fail
Ensure 'Prevent using Localhost IP address for WebRTC' is set to 'Enabled'	0	Fail
Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'	0	Fail
Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled'	0	Fail
Ensure 'Disable all apps from Windows Store' is set to 'Disabled'	0	Fail
Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled'	0	Fail
Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled'	0	Fail
Ensure 'Turn off the Store application' is set to 'Enabled'	0	Fail
Ensure 'Join Microsoft MAPS' is set to 'Disabled'	1	Pass
Ensure 'Configure Watson events' is set to 'Disabled'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Administrative Template

Rule Name	Score	Pass / Fail
Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled'	0	Fail
Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On'	0	Fail
Ensure 'Configure Windows spotlight on Lock Screen' is set to Disabled'	0	Fail
Ensure 'Do not suggest third-party content in Windows spotlight' is set to 'Enabled'	0	Fail
Ensure 'Turn off all Windows spotlight features' is set to 'Enabled'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: App runtime Rules

Rule Name	Score	Pass / Fail
Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'	0	Fail
Ensure 'Block launching Windows Store apps with Windows Runtime API access from hosted content.' is set to 'Enabled'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: User Account Control R

Rule Name	Score	Pass / Fail
Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled'	0	Fail
Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled'	1	Pass
Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'	0	Fail
Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	0	Fail
Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'	1	Pass
Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'	1	Pass
Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled'	1	Pass
Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'	1	Pass

Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (CCE Reference : CCE-35459-7)	1	Pass

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: AutoPlay Policies Rules

Rule Name	Score	Pass / Fail
Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	0	Fail
Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'	0	Fail
Ensure 'Turn off Autoplay' is set to 'Enabled: All drives'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: EMET Rules

Rule Name	Score	Pass / Fail
Ensure EMET is installed	0	Fail
Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'	0	Fail
Ensure 'Default Protections for Popular Software' is set to 'Enabled'	0	Fail
Ensure 'Default Protections for Recommended Software' is set to 'Enabled'	0	Fail
Set 'System ASLR' to 'Enabled:Application Opt-In'	0	Fail
Set 'System DEP' to 'Enabled:Application Opt-Out'	0	Fail
Set 'System SEHOP' to 'Enabled:Application Opt-Out'	0	Fail

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Account Policies - User

Rule Name	Score	Pass / Fail
Ensure 'Log on as a service' is set to 'No One'	0	Fail
Ensure 'Log on as a batch job' is set to 'Administrators'	0	Fail
Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'	1	Pass
Ensure 'Access this computer from the network' is set to 'Administrators, Remote Desktop Users'	0	Fail
Ensure 'Act as part of the operating system' is set to 'No One'	1	Pass
Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	0	Fail
Ensure 'Allow log on locally' is set to 'Administrators, Users'	0	Fail
Ensure 'Allow log on through Remote Desktop Services' is set to 'Administrators, Remote Desktop Users'	1	Pass
Ensure 'Back up files and directories' is set to 'Administrators'	0	Fail
Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	1	Pass
Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE, Users'	1	Pass
Ensure 'Create a pagefile' is set to 'Administrators'	1	Pass
Ensure 'Create a token object' is set to 'No One'	1	Pass
Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	1	Pass
Ensure 'Create permanent shared objects' is set to 'No One'	1	Pass
Configure 'Create symbolic links'	1	Pass
Ensure 'Debug programs' is set to 'Administrators'	1	Pass
Ensure 'Enable computer and user accounts to be trusted for delegation' is set to 'No One'	1	Pass

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Account Policies - User

Rule Name	Score	Pass / Fail
Ensure 'Force shutdown from a remote system' is set to 'Administrators'	1	Pass
Ensure 'Impersonate a client after authentication' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'	0	Fail
Ensure 'Increase scheduling priority' is set to 'Administrators'	1	Pass
Ensure 'Load and unload device drivers' is set to 'Administrators'	1	Pass
Ensure 'Lock pages in memory' is set to 'No One'	1	Pass
Ensure 'Modify an object label' is set to 'No One'	1	Pass
Ensure 'Modify firmware environment values' is set to 'Administrators'	1	Pass
Ensure 'Perform volume maintenance tasks' is set to 'Administrators'	1	Pass
Ensure 'Profile single process' is set to 'Administrators'	1	Pass
Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	1	Pass
Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'	0	Fail
Ensure 'Restore files and directories' is set to 'Administrators'	0	Fail

Ensure 'Shut down the system' is set to 'Administrators, Users'	0	Fail
Ensure 'Take ownership of files or other objects' is set to 'Administrators'	1	Pass

General System Hardening - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Windows Update Rules

Rule Name	Score	Pass / Fail
Ensure 'Configure Automatic Updates' is set to 'Enabled'	0	Fail
Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'	0	Fail
Set 'Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box' to 'Disabled'	0	Fail
Set 'Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box' to 'Disabled'	0	Fail
Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'	0	Fail
Set 'Reschedule Automatic Updates scheduled installations' to 'Enabled:1 minute'	0	Fail
Ensure 'Select when Feature Updates are received' is set to 'Enabled: Current Branch for Business, 180 or more days'	0	Fail
Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days'	0	Fail

HIPAA Standard: Non-Default Services List - Implement policies and procedures that specify the proper functions to be performed, the manner in which those functior

Non-Default Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any Non-Defau

Rule Name	Score	Pass / Fail
Check for any Non-Default Services	0	Fail

Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mar

Rule Name	Score	Pass / Fail
AllJoyn Router Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
App Readiness Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Application Host Helper Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Application Identity Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Application Information Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Application Layer Gateway Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Application Management Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
AppX Deployment Service (AppXSVC) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
ASP.NET State Service (aspnet_state) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
ActiveX Installer (AxInstSV) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Auto Time Zone Updater (tzautoupdate) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Background Intelligent Transfer Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	0	Fail
Background Tasks Infrastructure (BrokerInfrastructure) Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass

Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mar

Rule Name	Score	Pass / Fail
Base Filtering Engine Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Bluetooth Support Service (bthserv) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
CDPUserSvc (cdpusersvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Certificate Propagation Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Client License Service (ClipSVC) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
CNG Key Isolation Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
COM+ Event System Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
COM+ System Application Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Computer Browser Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Connected Devices Platform Service (CDPSvc) Service (Hardened Start Mode: Automatic, Hardened Expected State: Running, Stopped)	1	Pass
Connected User Experiences and Telemetry (DiagTrack) Service (Hardened Start Mode: Automatic, Hardened Expected State: Running)	1	Pass
Contact Data (PimIndexMaintenanceSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
CoreMessaging (CoreMessagingRegistrar) Service (Hardened Start Mode: Automatic, Hardened Expected State: Running)	1	Pass
Credential Manager Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Cryptographic Services Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Data Sharing (DsSvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass

Data Sharing (DcpSvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
DCOM Server Process Launcher Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Device Association (deviceassociationservice) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Device Install (DeviceInstall) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Device Management Enrollment (DmEnrollmentSvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Device Setup (DsmSvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
DevQuery Background Discovery Broker (DevQueryBroker) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
DHCP Client Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mar		
Rule Name	**Score**	**Pass / Fail**
Diagnostic Policy Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Diagnostic Service Host Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Diagnostic System Host Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Distributed Link Tracking Client Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Distributed Transaction Coordinator Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
DMWAPPushService (dmwappushservice) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
DNS Client Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Downloaded Maps Manager (MapsBroker) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Embedded Mode (embeddedmode) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
The Enhanced Mitigation Experience Toolkit (EMET) Service (Hardened Start Mode: Manual, Hardened Expected State: Running)	1	Pass
Encrypting File System (EFS) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Enterprise App Management (EntAppSvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Extensible Authentication Protocol Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Function Discovery Provider Host Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Function Discovery Resource Publication Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Geolocation (lfsvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Group Policy Client Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Human Interface Device Access Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mar		
Rule Name	**Score**	**Pass / Fail**
HV Host (HvHost) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Hyper-V Data Exchange Service (vmickvpexchange) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Hyper-V Guest Service Interface (vmicguestinterface) Service (Hardened Start Mode: Manual, Hardened Expected State: Running, Stopped)	1	Pass
Hyper-V Guest Shutdown Service (vmicshutdown) Service (Hardened Start Mode: Manual, Hardened Expected State: Running, Stopped)	1	Pass
Hyper-V Heartbeat Service (vmicheartbeat) Service (Hardened Start Mode: Manual, Hardened Expected State: Running, Stopped)	1	Pass
Hyper-V PowerShell Direct Service (vmicvmsession) Service (Hardened Start Mode: Manual, Hardened Expected State: Running, Stopped)	1	Pass
Hyper-V Remote Desktop Virtualization Service (vmicrdv) Service (Hardened Start Mode: Manual, Hardened Expected State: Running, Stopped)	1	Pass
Hyper-V Time Synchronization Service (vmictimesync) Service (Hardened Start Mode: Manual, Hardened Expected State: Running, Stopped)	1	Pass
Hyper-V Volume Shadow Copy Requestor (vmicvss) Service (Hardened Start Mode: Manual, Hardened Expected State: Running, Stopped)	1	Pass
IKE and AuthIP IPsec Keying Modules Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	0	Fail
Interactive Services Detection Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Internet Connection Sharing (ICS) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
IP Helper Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
IPsec Policy Agent Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
KDC Proxy Server service (KPSSVC) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
KtmRm for Distributed Transaction Coordinator Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Link-Layer Topology Discovery Mapper Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Local Session Manager Service (Hardened Start Mode: Automatic, Hardened Expected State: Running)	1	Pass
Microsoft (R) Diagnostics Hub Standard Collector Service (diagnosticshub.standardcollector.service) Service (Hardened Start Mode: Manual, Hardened Expected Sta	1	Pass
Microsoft App-V Client Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Microsoft Account Sign-in Assistant Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail

Microsoft iSCSI Initiator Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Microsoft Passport (NgcSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Microsoft Passport Container (NgcCtnrSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Microsoft Software Shadow Copy Provider Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Microsoft Storage Spaces SMP (smphost) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Net.Tcp Port Sharing Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Netlogon Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Network Access Protection Agent Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Network Connections Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Network Connectivity Assistant (ncasvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Network List Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Network Location Awareness Service (Hardened Start Mode: Auto, Hardened Expected State: Stopped, Running)	1	Pass
Network Setup (NetSetupSvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Network Store Interface Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Offline Files (CscService) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Optimize Drives (defragsvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Performance Counter DLL Host (PerfHost) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Performance Logs and Alerts Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Phone (PhoneSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Plug and Play Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Portable Device Enumerator (WPDBusEnum) Service Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Power Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Print Spooler Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mar		
Rule Name	**Score**	**Pass / Fail**
Printer Extensions and Notifications (PrintNotify) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Problem Reports and Solutions Control Panel Support Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Program Compatibility Assistant (PcaSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Quality Windows Audio Video Experience (QWAVE) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Radio Management Service (RmSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Remote Access Auto Connection Manager Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Remote Access Connection Manager Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Remote Desktop Configuration Service (Hardened Start Mode: Disabled, Hardened Expected State: Running)	0	Fail
Remote Desktop Services Service (Hardened Start Mode: Disabled, Hardened Expected State: Running)	0	Fail
Remote Desktop Services UserMode Port Redirector (Hardened Start Mode: Disabled, Hardened Expected State: Running)	0	Fail
Remote Procedure Call (RPC) Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Remote Procedure Call (RPC) Locator Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Remote Registry Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped/Running)	0	Fail
Resultant Set of Policy Provider Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Routing and Remote Access Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
RPC Endpoint Mapper Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Secondary Logon Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Secure Socket Tunneling Protocol Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Security Accounts Manager Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Sensor Data Service (SensorDataService) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Sensor Monitoring Service (SensrSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Sensor Service (SensorService) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Server Service (Hardened Start Mode: Disabled, Hardened Expected State: Running)	0	Fail
Shell Hardware Detection Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mar		
Rule Name	**Score**	**Pass / Fail**

Smart Card Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Smart Card Device Enumeration (ScDeviceEnum) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Smart Card Removal Policy (SCPolicySvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
SNMP Trap Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Software Protection Service (Hardened Start Mode: Auto, Hardened Expected State: Stopped, Running)	1	Pass
Special Administration Console Helper Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Spot Verifier Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
SSDP Discovery Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
State Repository (StateRepository) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Still Image Acquisition Events (WiaRpc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Storage (StorSvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Storage Tiers Management Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Superfetch Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Sync Host (OneSyncSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
System Event Notification Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
System Events Broker Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Task Scheduler Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
TCP/IP NetBIOS Helper Service (Hardened Start Mode: Manual, Hardened Expected State: Running)	1	Pass
Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mar		
Rule Name	**Score**	**Pass / Fail**
Telephony Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Themes Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Tile Data model server Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Time Broker (TimeBrokerSvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Touch Keyboard and Handwriting Panel Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Update Orchestrator Service for Windows Update (UsoSvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
UPnP Device Host Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
User Access Logging Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
User Data Access (UserDataSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
User Data Storage (UnistoreSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
User Experience Virtualization (UevAgentService) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
User Manager (UserManager) Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
User Profile (ProfSvc) Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Virtual Disk Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Volume Shadow Copy Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
WalletService (WalletService) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Windows Audio Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Windows Audio Endpoint Builder Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Windows Biometric Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Windows Connection Manager (wcmsvc) Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Windows Camera Frame (FrameServer) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Windows Defender Network Inspection (WdNisSvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped/Running)	1	Pass
Windows Defender (WinDefend) Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Windows Driver Foundation - User-mode Driver Framework (wudfsvc) Service (Hardened Start Mode: Manual, Hardened Expected State: Running/Stopped)	1	Pass
Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mar		
Rule Name	**Score**	**Pass / Fail**
Windows Encryption Provider Host (WEPHOSTSVC) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Windows Error Reporting (WerSvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Running/Stopped)	0	Fail
Windows Event Collector (Wecsvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Running/Stopped)	0	Fail
Windows Event Log (EventLog) Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Windows Firewall (MpsSvc) Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass

Windows Font Cache (FontCache) Service (Hardened Start Mode: Auto, Hardened Expected State: Stopped, Running)	1	Pass
Windows Image Acquisition (WIA) (stisvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Windows Insider (wisvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Windows Installer Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Windows License Manager (LicenseManager) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Windows Management Instrumentation Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Windows Mobile Hotspot Service (icssvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Windows Modules Installer Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Windows Push Notifications System (WpnService) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Windows Push Notifications User (WpnUserService) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Windows Presentation Foundation Font Cache (FontCache3.0.0.0) Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Windows Remote Management (WS-Management) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped, Running)	0	Fail
Windows Search (WSearch) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	1	Pass
Mandatory Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Mar		
Rule Name	**Score**	**Pass / Fail**
Windows Time Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Windows Update Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped/Running)	1	Pass
WinHTTP Web Proxy Auto-Discovery (WinHttpAutoProxySvc) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped/Running)	0	Fail
Wired AutoConfig Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
WMI Performance Adapter Service (Hardened Start Mode: Manual, Hardened Expected State: Stopped, Running)	1	Pass
Workstation Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Xbox Live Auth Manager (XblAuthManager) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Xbox Live Game Save (XblGameSave) Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
HIPAA Standard: Optional Services List - Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions a		
Optional Services List - Identify Workstation Types and Functions or Uses, Identify Expected Performance of Each Type of Workstation: Check for any missing Optior		
Rule Name	**Score**	**Pass / Fail**
Optional Services List: NNT ChangeTracker Gen7 Agent (Gen7Agent) (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Optional Services List: NNT Change Tracker Gen 7 MongoDB Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Optional Services List: NNT Change Tracker Gen 7 Redis Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	1	Pass
Optional Services List: ASP.NET State Service (aspnet_state) Service (Hardened Start Mode: Auto, Hardened Expected State: Running)	0	Fail
Optional Services List: World Wide Web Publishing Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
Optional Services List: W3C Logging Service (Hardened Start Mode: Disabled, Hardened Expected State: Stopped)	0	Fail
4.12. Workstation Security (§ 164.310(c))		
HIPAA Standard: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.		
Identify All Methods of Physical Access to Workstations, Analyze the Risk Associated with Each Type of Access, Identify and Implement Physical Safeguards for Wor		
Rule Name	**Score**	**Pass / Fail**
Document the different ways workstations are accessed by employees and nonemployees, Determine which type of access holds the greatest threat to security, Imple	1	Pass
4.13. Device and Media Controls (§ 164.310(d)(1))		
HIPAA Standard: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health in		
Implement Procedures for Reuse of Electronic Media - Security parameters to prevent misuse: Account Policies - Devices Rules		
Rule Name	**Score**	**Pass / Fail**
Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users'	0	Fail
Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'	1	Pass
4.14. Access Control (§ 164.312(a)(1))		
HIPAA Standard: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access		
Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Remote Desktop Rules		
Rule Name	**Score**	**Pass / Fail**
Ensure 'Allow users to connect remotely by using Remote Desktop Services' is set to 'Disabled' (CCE Reference : CCE-35255-9)	0	Fail
Ensure 'Do not allow COM port redirection' is set to 'Enabled'	0	Fail

Ensure 'Do not allow LPT port redirection' is set to 'Enabled'	0	Fail
Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled'	0	Fail
Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less'	0	Fail
Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute'	0	Fail
Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	0	Fail
Ensure 'Do not allow drive redirection' is set to 'Enabled'	0	Fail
Ensure 'Always prompt for password upon connection' is set to 'Enabled'	0	Fail

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Remote Desktop Rules

Rule Name	Score	Pass / Fail
Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'	0	Fail
Ensure 'Require secure RPC communication' is set to 'Enabled'	0	Fail
Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'	0	Fail
Ensure 'Do not use temporary folders per session' is set to 'Disabled'	0	Fail

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Windows Logon Options Rules

Rule Name	Score	Pass / Fail
Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled'	1	Pass

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Windows Remote Management (WinR

Rule Name	Score	Pass / Fail
Ensure 'Allow Basic authentication' is set to 'Disabled'	0	Fail
Ensure 'Allow unencrypted traffic' is set to 'Disabled'	0	Fail
Ensure 'Disallow Digest authentication' is set to 'Enabled'	0	Fail
Ensure 'Allow Basic authentication' is set to 'Disabled'	0	Fail
Ensure 'Allow remote server management through WinRM' is set to 'Disabled'	0	Fail
Ensure 'Allow unencrypted traffic' is set to 'Disabled'	0	Fail
Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'	0	Fail

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Firewall configuration standards: Win

Rule Name	Score	Pass / Fail
Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	0	Fail
Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	0	Fail
Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	0	Fail
Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (CCE Reference : CCE-33062-1)	0	Fail
Set 'Windows Firewall: Domain: Allow unicast response' to 'No'	0	Fail
Set 'Windows Firewall: Domain: Apply local firewall rules' to 'Yes (default)'	0	Fail
Set 'Windows Firewall: Domain: Apply local connection security rules' to 'Yes (default)'	0	Fail
Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'	0	Fail
Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	0	Fail
Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	0	Fail
Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes'	0	Fail

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Firewall configuration standards: Win

Rule Name	Score	Pass / Fail
Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'	0	Fail
Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'	0	Fail
Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	0	Fail
Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (CCE Reference : CCE-33065-4)	0	Fail
Set 'Windows Firewall: Private: Allow unicast response' to 'No'	0	Fail
Set 'Windows Firewall: Private: Apply local firewall rules' to 'Yes (default)'	0	Fail
Set 'Windows Firewall: Private: Apply local connection security rules' to 'Yes (default)'	0	Fail
Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log'	0	Fail
Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	0	Fail
Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'	0	Fail
Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'	0	Fail

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Firewall configuration standards: Win

Rule Name	Score	Pass / Fail
Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'	0	Fail
Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)'	0	Fail

Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'	0	Fail
Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'No' (CCE Reference : CCE-33068-8)	0	Fail
Set 'Windows Firewall: Public: Allow unicast response' to 'No'	0	Fail
Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	0	Fail
Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'	0	Fail
Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	0	Fail
Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'	0	Fail
Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	0	Fail
Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	0	Fail

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Security parameters to prevent misus

Rule Name	Score	Pass / Fail
Ensure 'Accounts: Administrator account status' is set to 'Disabled'	0	Fail
Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'	0	Fail
Ensure 'Accounts: Guest account status' is set to 'Disabled'	1	Pass
Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	1	Pass
Configure 'Accounts: Rename administrator account'	0	Fail
Configure 'Accounts: Rename guest account'	0	Fail

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Network Access Rules

Rule Name	Score	Pass / Fail
Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	1	Pass
Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'	1	Pass
Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	0	Fail
Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'	0	Fail
Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	1	Pass
Ensure 'Network access: Named Pipes that can be accessed anonymously' is set to 'None'	1	Pass
Ensure 'Network access: Remotely accessible registry paths'	1	Pass
Ensure 'Network access: Remotely accessible registry paths and sub-paths'	1	Pass
Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'	1	Pass
Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow'	0	Fail
Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	1	Pass
Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'	1	Pass

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Network Security Rules

Rule Name	Score	Pass / Fail
Ensure 'Do not display network selection UI' is set to 'Enabled'	0	Fail
Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'	0	Fail
Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled'	0	Fail
Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'	0	Fail
Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled'	0	Fail
Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled'	0	Fail
Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated'	0	Fail

Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Network Security Rules

Rule Name	Score	Pass / Fail
Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'	0	Fail
Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	0	Fail
Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	0	Fail
Ensure 'Prevent the computer from joining a homegroup' is set to 'Enabled'	0	Fail
Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	0	Fail
Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'	0	Fail
Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'	1	Pass

Ensure 'Deny access to this computer from the network' to include 'Guests, Local account'	0	Fail
Ensure 'Deny log on as a batch job' to include 'Guests'	0	Fail
Ensure 'Deny log on as a service' to include 'Guests'	0	Fail
Ensure 'Deny log on locally' to include 'Guests'	0	Fail
Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'	0	Fail
Ensure 'Enable Font Providers' is set to 'Disabled'	0	Fail
Ensure 'Enable insecure guest logons' is set to 'Disabled'	0	Fail
Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'	0	Fail
Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'	0	Fail
Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'	0	Fail
Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'	0	Fail
Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'	0	Fail
Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	0	Fail
Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled'	0	Fail
Implement technical policies to allow access only to those persons or software programs that have been granted access rights - Network Security Rules		
Rule Name	**Score**	**Pass / Fail**
Ensure 'Enable/Disable PerfTrack' is set to 'Disabled'	0	Fail
Ensure 'Use enhanced anti-spoofing when available' is set to 'Enabled'	0	Fail
Ensure 'Prevent downloading of enclosures' is set to 'Enabled'	0	Fail

4.15. Audit Controls (§ 164.312(b))

HIPAA Standard: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electroni

Select the Tools that Will Be Deployed for Auditing and System Activity Reviews

Rule Name	**Score**	**Pass / Fail**
Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	0	Fail
2.2.23 (L1) Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	0	Fail
Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	0	Fail
Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	1	Pass

Develop Appropriate Standard Operating Procedures: Windows Components - Event Log Rules

Rule Name	**Score**	**Pass / Fail**
Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	0	Fail
Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	0	Fail
Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	0	Fail
Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	0	Fail
Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	0	Fail
Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	0	Fail
Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'	0	Fail
(L1) Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	0	Fail

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - System Rules

Rule Name	**Score**	**Pass / Fail**
Ensure 'Audit System Integrity' is set to 'Success and Failure'	1	Pass
Ensure 'Audit Security System Extension' is set to 'Success and Failure'	0	Fail
Ensure 'Audit Security State Change' is set to 'Success' (CCE Reference : CCE-33043-1)	1	Pass
Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	0	Fail
Ensure 'Audit IPsec Driver' is set to 'Success and Failure'	0	Fail

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Object Access Rules

Rule Name	**Score**	**Pass / Fail**
Set 'Audit Policy: Object Access: Handle Manipulation' to 'No Auditing'	1	Pass
Set 'Audit Policy: Object Access: Other Object Access Events' to 'No Auditing'	1	Pass

Set 'Audit Policy: Object Access: File Share' to 'No Auditing'	1	Pass
Set 'Audit Policy: Object Access: File System' to 'No Auditing'	1	Pass
Set 'Audit Policy: Object Access: SAM' to 'No Auditing'	1	Pass
Set 'Audit Policy: Object Access: Kernel Object' to 'No Auditing'	1	Pass
Set 'Audit Policy: Object Access: Filtering Platform Packet Drop' to 'No Auditing'	1	Pass
Set 'Audit Policy: Object Access: Registry' to 'No Auditing'	1	Pass
Set 'Audit Policy: Object Access: Certification Services' to 'No Auditing'	1	Pass
Set 'Audit Policy: Object Access: Application Generated' to 'No Auditing'	1	Pass
Set 'Audit Policy: Object Access: Detailed File Share' to 'No Auditing'	1	Pass
Set 'Audit Policy: Object Access: Filtering Platform Connection' to 'No Auditing'	1	Pass
Ensure 'Audit Removable Storage' is set to 'Success and Failure'	0	Fail

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Logon-Logoff Rules

Rule Name	Score	Pass / Fail
Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'	0	Fail
Ensure 'Audit Special Logon' is set to 'Success'	1	Pass
Set 'Audit Policy: Logon-Logoff: IPsec Main Mode' to 'No Auditing'	1	Pass
Ensure 'Audit Account Lockout' is set to 'Success and Failure'	0	Fail
Ensure 'Audit Group Membership' is set to 'Success'	0	Fail
Set 'Audit Policy: Logon-Logoff: IPsec Extended Mode' to 'No Auditing'	1	Pass
Set 'Audit Policy: Logon-Logoff: IPsec Quick Mode' to 'No Auditing'	1	Pass
Ensure 'Audit Logoff' is set to 'Success'	1	Pass
Set 'Audit Policy: Logon-Logoff: Network Policy Server' to 'No Auditing'	0	Fail
Ensure 'Audit Logon' is set to 'Success and Failure'	1	Pass

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - DS Access Rules

Rule Name	Score	Pass / Fail
Set 'Audit Policy: DS Access: Directory Service Replication' to 'No Auditing'	1	Pass
Set 'Audit Policy: DS Access: Detailed Directory Service Replication' to 'No Auditing'	1	Pass
Set 'Audit Policy: DS Access: Directory Service Changes' to 'No Auditing'	1	Pass
Set 'Audit Policy: DS Access: Directory Service Access' to 'No Auditing'	0	Fail

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Detailed Tracking Rules

Rule Name	Score	Pass / Fail
Set 'Audit Policy: Detailed Tracking: DPAPI Activity' to 'No Auditing'	1	Pass
Set 'Audit Policy: Detailed Tracking: Process Termination' to 'No Auditing'	1	Pass
Ensure 'Audit PNP Activity' is set to 'Success'	0	Fail
Ensure 'Audit Process Creation' is set to 'Success' (CCE Reference : CCE-33040-7)	0	Fail
Set 'Audit Policy: Detailed Tracking: RPC Events' to 'No Auditing'	1	Pass

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Policy Change Rules

Rule Name	Score	Pass / Fail
Set 'Audit Policy: Policy Change: MPSSVC Rule-Level Policy Change' to 'No Auditing'	1	Pass
Set 'Audit Policy: Policy Change: Filtering Platform Policy Change' to 'No Auditing'	1	Pass
Ensure 'Audit Authorization Policy Change' is set to 'Success'	0	Fail
Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'	0	Fail
Set 'Audit Policy: Policy Change: Other Policy Change Events' to 'No Auditing'	1	Pass
Ensure 'Audit Authentication Policy Change' is set to 'Success'	1	Pass

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Account Management Rules

Rule Name	Score	Pass / Fail

Set 'Audit Policy: Account Management: Distribution Group Management' to 'No Auditing'	1	Pass
Ensure 'Audit Computer Account Management' is set to 'Success and Failure'	0	Fail
Ensure 'Audit Computer Account Management' is set to 'Success and Failure'	0	Fail
Ensure 'Audit Security Group Management' is set to 'Success and Failure'	0	Fail
Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'	0	Fail
Ensure 'Audit Application Group Management' is set to 'Success and Failure'	0	Fail

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Account Logon Rules

Rule Name	Score	Pass / Fail
Set 'Audit Policy: Account Logon: Kerberos Authentication Service' to 'No Auditing'	0	Fail
Set 'Audit Policy: Account Logon: Other Account Logon Events' to 'No Auditing'	1	Pass
Set 'Audit Policy: Account Logon: Kerberos Service Ticket Operations' to 'No Auditing'	0	Fail
Ensure 'Audit Credential Validation' is set to 'Success and Failure'	0	Fail

Develop Appropriate Standard Operating Procedures: Advanced Audit Policy Configuration - Privilege Use Rules

Rule Name	Score	Pass / Fail
Set 'Audit Policy: Privilege Use: Other Privilege Use Events' to 'No Auditing'	1	Pass
Set 'Audit Policy: Privilege Use: Non Sensitive Privilege Use' to 'No Auditing'	1	Pass
Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'	0	Fail

4.16. Integrity (§ 164.312(c)(1))

HIPAA Standard: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Develop and Implement the Integrity Policy and Requirements: Anti-Virus Protection Check

Rule Name	Score	Pass / Fail
Verify Virus Protection is enabled and updated	1	Pass

Develop and Implement the Integrity Policy and Requirements: Protect all systems against malware - Early Launch Antimalware Rules

Rule Name	Score	Pass / Fail
Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'	0	Fail

Develop and Implement the Integrity Policy and Requirements: Protect all systems against malware - Attachment Rules

Rule Name	Score	Pass / Fail
Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'	0	Fail

5 - 6. Implement a Mechanism to Authenticate EPHI and a Monitoring Process To Assess How the Implemented Process Is Working

Rule Name	Score	Pass / Fail
Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.	1	Pass

Develop and Implement the Integrity Policy and Requirements: Use Data Encryption to Protect EPHI

Rule Name	Score	Pass / Fail
(BL) Ensure 'Interactive logon: Machine account lockout threshold' is set to '10 or fewer invalid logon attempts, but not 0'	0	Fail
(BL) Ensure 'Prevent installation of devices that match any of these device IDs' is set to 'Enabled'	0	Fail
(BL) Ensure 'Prevent installation of devices that match any of these device IDs: Prevent installation of devices that match any of these device IDs' is set to 'PCI\CC_0(	0	Fail
(BL) Ensure 'Prevent installation of devices that match any of these device IDs: Also apply to matching devices that are already installed.' is set to 'True' (checked)	0	Fail
(BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes' is set to 'Enabled'	0	Fail
(BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes: Prevent installation of devices using drivers for these device setup' is	0	Fail
(BL) Ensure 'Prevent installation of devices using drivers that match these device setup classes: Also apply to matching devices that are already installed.' is set to 'Tr	0	Fail
(BL) Ensure 'Allow standby states (S1-S3) when sleeping (on battery)' is set to 'Disabled'	0	Fail
(BL) Ensure 'Allow standby states (S1-S3) when sleeping (plugged in)' is set to 'Disabled'	0	Fail
(BL) Ensure 'Allow access to BitLocker-protected fixed data drives from earlier versions of Windows' is set to 'Disabled'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered' is set to 'Enabled'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Allow data recovery agent' is set to 'Enabled: True'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Password' is set to 'Enabled: Allow 48-digit recovery password'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Recovery Key' is set to 'Enabled: Allow 256-bit recovery key'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Save BitLocker recovery information to AD DS for fixed data drives' is set to 'Enabled: Fa	0	Fail
(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Configure storage of BitLocker recovery information to AD DS' is set to 'Enabled: Backup	0	Fail
(BL) Ensure 'Choose how BitLocker-protected fixed drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for fixed data drive	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for fixed data drives' is set to 'Enabled'	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for fixed data drives: Use BitLocker software-based encryption when hardware encryption is not available' is	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for fixed data drives: Restrict encryption algorithms and cipher suites allowed for hardware-based encryption	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for fixed data drives: Restrict crypto algorithms or cipher suites to the following:' is set to 'Enabled: 2.16.840	0	Fail
(BL) Ensure 'Configure use of passwords for fixed data drives' is set to 'Disabled' (CCE Reference : CCE-33165-2)	0	Fail
(BL) Ensure 'Configure use of smart cards on fixed data drives' is set to 'Enabled'	0	Fail
(BL) Ensure 'Configure use of smart cards on fixed data drives: Require use of smart cards on fixed data drives' is set to 'Enabled: True'	0	Fail
(BL) Ensure 'Allow enhanced PINs for startup' is set to 'Enabled'	0	Fail
(BL) Ensure 'Allow Secure Boot for integrity validation' is set to 'Enabled'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered' is set to 'Enabled'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Allow data recovery agent' is set to 'Enabled: False'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Recovery Password' is set to 'Enabled: Require 48-digit recovery password'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Recovery Key' is set to 'Enabled: Do not allow 256-bit recovery key'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: Tr	0	Fail

Develop and Implement the Integrity Policy and Requirements: Use Data Encryption to Protect EPHI

Rule Name	Score	Pass / Fail
(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Save BitLocker recovery information to AD DS for operating system drives' i	0	Fail
(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Configure storage of BitLocker recovery information to AD DS:' is set to 'Ena	0	Fail
(BL) Ensure 'Choose how BitLocker-protected operating system drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for op	0	Fail

(BL) Ensure 'Configure minimum PIN length for startup' is set to 'Enabled: 7 or more characters'	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for operating system drives' is set to 'Enabled'	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for operating system drives: Use BitLocker software-based encryption when hardware encryption is not ava	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for operating system drives: Restrict encryption algorithms and cipher suites allowed for hardware-based er	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for operating system drives: Restrict crypto algorithms or cipher suites to the following:' is set to 'Enabled: 2	0	Fail
(BL) Ensure 'Configure use of passwords for operating system drives' is set to 'Disabled'	0	Fail
(BL) Ensure 'Require additional authentication at startup' is set to 'Enabled'	0	Fail
Develop and Implement the Integrity Policy and Requirements: Use Data Encryption to Protect EPHI		
Rule Name	**Score**	**Pass / Fail**
(BL) Ensure 'Require additional authentication at startup: Allow BitLocker without a compatible TPM' is set to 'Enabled: False'	0	Fail
(BL) Ensure 'Require additional authentication at startup: Configure TPM startup:' is set to 'Enabled: Do not allow TPM'	0	Fail
(BL) Ensure 'Require additional authentication at startup: Configure TPM startup PIN:' is set to 'Enabled: Require startup PIN with TPM'	0	Fail
(BL) Ensure 'Require additional authentication at startup: Configure TPM startup key:' is set to 'Enabled: Do not allow startup key with TPM'	0	Fail
(BL) Ensure 'Require additional authentication at startup: Configure TPM startup key and PIN:' is set to 'Enabled: Do not allow startup key and PIN with TPM'	0	Fail
(BL) Ensure 'Allow access to BitLocker-protected removable data drives from earlier versions of Windows' is set to 'Disabled'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered' is set to 'Enabled'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Allow data recovery agent' is set to 'Enabled: True'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Recovery Password' is set to 'Enabled: Do not allow 48-digit recovery password' ((	0	Fail
(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Recovery Key' is set to 'Enabled: Do not allow 256-bit recovery key'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Omit recovery options from the BitLocker setup wizard' is set to 'Enabled: True'	0	Fail
(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Save BitLocker recovery information to AD DS for removable data drives' is set to	0	Fail
(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Configure storage of BitLocker recovery information to AD DS:' is set to 'Enabled: I	0	Fail
(BL) Ensure 'Choose how BitLocker-protected removable drives can be recovered: Do not enable BitLocker until recovery information is stored to AD DS for removab	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for removable data drives' is set to 'Enabled'	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for removable data drives: Use BitLocker software-based encryption when hardware encryption is not availa	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for removable data drives: Restrict encryption algorithms and cipher suites allowed for hardware-based enc	0	Fail
(BL) Ensure 'Configure use of hardware-based encryption for removable data drives: Restrict crypto algorithms or cipher suites to the following:' is set to 'Enabled: 2.1	0	Fail
(BL) Ensure 'Configure use of passwords for removable data drives' is set to 'Disabled'	0	Fail
(BL) Ensure 'Configure use of smart cards on removable data drives' is set to 'Enabled'	0	Fail
(BL) Ensure 'Configure use of smart cards on removable data drives: Require use of smart cards on removable data drives' is set to 'Enabled: True'	0	Fail
(BL) Ensure 'Deny write access to removable drives not protected by BitLocker' is set to 'Enabled'	0	Fail
(BL) Ensure 'Deny write access to removable drives not protected by BitLocker: Do not allow write access to devices configured in another organization' is set to 'Enal	0	Fail
(BL) Ensure 'Choose drive encryption method and cipher strength (Windows 10 [Version 1511] and later)' is set to 'Enabled: XTS-AES 256-bit'	0	Fail
(BL) Ensure 'Disable new DMA devices when this computer is locked' is set to 'Enabled'	0	Fail

4.17. Person or Entity Authentication (§ 164.312(d))

HIPAA Standard: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Authentication - Security parameters to prevent misuse: Account Policies - Password Policy

Rule Name	Score	Pass / Fail
Ensure 'Enforce password history' is set to '24 or more password(s)'	0	Fail
Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'	1	Pass
Ensure 'Minimum password age' is set to '1 or more day(s)'	0	Fail
Ensure 'Minimum password length' is set to '14 or more character(s)'	0	Fail
Ensure 'Password must meet complexity requirements' is set to 'Enabled' (CCE Reference : CCE-33777-4)	1	Pass
Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	1	Pass

Authentication - Security parameters to prevent misuse: Account Policies - Account Lockout Rules

Rule Name	Score	Pass / Fail
Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0'	0	Fail
Ensure 'Account lockout duration' is set to '15 or more minute(s)'	0	Fail
Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)'	0	Fail
Set 'Network security: Force logoff when logon hours expire' to 'Enabled'	0	Fail
Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'	1	Pass
Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0'	1	Pass

Authentication - Security parameters to prevent misuse: Account Policies - Interactive logon Rules

Rule Name	Score	Pass / Fail
Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'	0	Fail
Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'	0	Fail
Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'	1	Pass
Configure 'Interactive logon: Message text for users attempting to log on' (CCE Reference : CCE-35064-5)	0	Fail
Configure 'Interactive logon: Message title for users attempting to log on' (CCE Reference : CCE-35179-1)	0	Fail
Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)'	0	Fail
Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'	1	Pass
Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only)	0	Fail
Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	0	Fail

Authentication - Security parameters to prevent misuse: Account Policies - MSS Rules

Rule Name	Score	Pass / Fail
Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	0	Fail
Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds	0	Fail
Ensure 'MSS: (DisableSavePassword) Prevent the dial-up password from being saved' is set to 'Enabled'	0	Fail
Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routir	0	Fail
Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is (	0	Fail
Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	0	Fail
Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)'	0	Fail
Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'	0	Fail
Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled'	0	Fail
Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'	0	Fail
Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'	0	Fail
Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'	0	Fail
Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	0	Fail

Authentication - Security parameters to prevent misuse: Account Policies - Recovery console Rules

Rule Name	Score	Pass / Fail
Set 'Recovery console: Allow automatic administrative logon' to 'Disabled'	1	Pass
Set 'Recovery console: Allow floppy copy and access to all drives and all folders' to 'Disabled'	1	Pass

Authentication -Security parameters to prevent misuse: Account Policies - Shutdown Rules

Rule Name	Score	Pass / Fail
Set 'Shutdown: Allow system to be shut down without having to log on' to 'Disabled'	1	Pass

Authentication -Security parameters to prevent misuse: Account Policies - System objects Rules

Rule Name	Score	Pass / Fail
Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (CCE Reference : CCE-35008-2)	1	Pass
Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled'	1	Pass

4.18. Transmission Security (§ 164.312(e)(1))

HIPAA Standard: Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that

Transmission Security - Security parameters to prevent misuse: Account Policies - Domain member Rules

Rule Name	Score	Pass / Fail
Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'	1	Pass
Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'	1	Pass
Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'	1	Pass
Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'	1	Pass
Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'	1	Pass
Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'	1	Pass

Transmission Security - Security parameters to prevent misuse: Account Policies - Microsoft network client Rules

Rule Name	Score	Pass / Fail
Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	0	Fail
Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'	1	Pass
Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'	1	Pass

Transmission Security - Security parameters to prevent misuse: Account Policies - Microsoft network server Rules

Rule Name	Score	Pass / Fail
Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'	0	Fail
Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	0	Fail
Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher	0	Fail

Transmission Security - Use strong cryptography and security protocols

Rule Name	Score	Pass / Fail
Ensure 'System cryptography: Force strong key protection for user keys stored on the computer' is set to 'User is prompted when the key is first used' or higher	0	Fail
Set 'System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing' to 'Enabled'	0	Fail
Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM&NTLM'	0	Fail
Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher	1	Pass
Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit	0	Fail
Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bi	0	Fail
Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'	1	Pass