Windows 10 Configuration Standard

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*Classification: Internal*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX.; it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX.

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Industry Configuration Standards 3

1.5 Related Documents / References 3

2. Standard Statements 4

2.1 User account hardening 4

2.2 Authentication policy 5

2.3 Active Directory 6

2.4 System hardening 6

2.5 Windows Defender configuration 10

2.6 AppLocker configuration 11

2.7 BitLocker configuration 15

2.8 Windows Defender Exploit Guard configuration 16

2.9 Windows Defender Device Guard and Application Control configuration 17

2.10 Windows Defender Application Guard configuration 18

2.11 Windows Defender Firewall configuration 20

2.12 VPN configuration 22

2.13 Management of UEFI firmware settings 23

2.14 Windows 10 Enterprise feature updates 24

3. Standard Compliance & Enforcement 25

3.1 Compliance Measures 25

3.2 Enforcement 25

4. Exception Process / Glossary 26

4.1 Exception Process 26

4.2 Glossary / Acronyms 26

5. Document Management 27

5.1 Document Revision Log 27

5.2 Document Ownership 27

5.3 Document Coordinator 27

5.4 Document Approvers 27

5.5 Distribution 27

# Introduction

## Document Definition

This document is a Standard.

For a full description of document types, see XXXX-POL-ALL-001 - Information Security Policy Framework.

## Objective

The objective of this standard is to ensure the XXXXs business and technical requirements for the windows 10 operating system are translated into a baseline that will allow administrators to easily configure the operating system to adequately protect the XXXX’s information assets against external and internal threats.

## Scope

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Standard applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Standard statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Standard applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Industry Configuration Standards

* Centre for Internet Security (CIS): http://www.cisecurity.org/
* National Cyber Security Centre: End user device (EUD) security guidance

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*

# Standard Statements

## User account hardening

| **Group Policy** | **Value(s)** |
| --- | --- |
| Computer Configuration > Administrative Templates > Network > Network Connections > Require domain users to elevate when setting a network’s location | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Credential User Interface > Do not display the password reveal button | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > OneDrive > Prevent the usage of OneDrive for file storage | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Sync your settings > Do not sync | Enabled  Allow users to turn syncing on: Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Search > Allow Cortana | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Search > Don’t search the web or display web results in Search | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Store > Disable all apps from Microsoft Store | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Store > Turn off Automatic Download and Install of updates | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Store > Turn off the Store application | Enabled |
| User Configuration > Administrative Templates > Control Panel > Personalization > Screen saver timeout | 600 seconds |
| Computer Configuration > Administrative Templates > System > Logon > Turn off picture password sign-in | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Hello for Business > Use a hardware security device | Enabled |

## Authentication policy

| **Group Policy** | **Value(s)** |
| --- | --- |
| CN=System > CN=Password Settings Container > CN=Granular Password Settings Users | Precedence: 2  Enforce minimum password length  Enforce lockout policy  Account will be locked out: Until an administrator manually unlocks the account  Directly Applies To: Domain Users |
| CN=System > CN=Password Settings Container > CN=Granular Password Settings Administrators | Precedence: 1  Enforce minimum password length  Password must meet complexity requirements  Enforce lockout policy  Account will be locked out: Until an administrator manually unlocks the account  Directly Applies To: Domain Admins  Protect from accidental deletion: Enabled |

## Active Directory

|  |
| --- |
| **Group Policy > Computer Configuration > Administrative Templates > System > PIN Complexity** |
| PIN Complexity > Maximum PIN length |
| PIN Complexity > Minimum PIN length |
| PIN Complexity > Require digits |
| PIN Complexity > Require lowercase letters |
| PIN Complexity > Require special characters |
| PIN Complexity > Require uppercase characters |

## System hardening

|  |  |
| --- | --- |
| **Group Policy** | **Value(s)** |
| Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Allow Telemetry | Enabled:  0 - Security  Note - If using Windows Update for Business this will need to be set to 1 (Basic). |
| Computer Configuration > Administrative Templates > Windows Components > Windows Error Reporting > Disable Windows Error Reporting | Enabled |
| Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions > Prevent installation of devices that match these device IDs | Enabled: PCI\CC\_0C0A  Also apply to matching devices that are already installed: Disabled |
| Computer Configuration > Administrative Templates > System > Device Installation > Device Installation Restrictions > Prevent installation of drivers matching these device setup classes | Enabled:  {d48179be-ec20-11d1-b6b8-00c04fa372a7}  {7ebefbc0-3200-11d2-b4c2-00a0C9697d07}  {c06ff265-ae09-48f0-812c-16753d7cba83}  {6bdd1fc1-810f-11d0-bec7-08002be2092f}  Also apply to matching devices that are already installed: Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Store > Turn off Automatic Download and Install of updates | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > App runtime > Block launching Universal Windows apps with Windows Runtime API access from hosted content. | Enabled |
| Computer Configuration > Administrative Templates > Network > Network Isolation > Proxy definitions are authoritative | Enabled |
| Computer Configuration > Administrative Templates > Network > Network Isolation > Subnet definitions are authoritative | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Portable Operating System > Windows To Go Default Startup Options | Disabled |
| Computer Configuration > Preferences > Windows Settings > Registry > Replace > HKLM\Software\Microsoft\Windows\CurrentVersion\policies\system\ | (DWORD) SafeModeBlockNonAdmins = 1 |
| Computer Configuration > Preferences > Windows Settings > Registry > Replace > HKLM\System\CurrentControlSet\Control\SafeBoot\Network | (REG\_SZ)  Appid = Service |
| Computer Configuration > Preferences > Windows Settings > Registry > Replace > HKLM\System\CurrentControlSet\Control\SafeBoot\Network | (REG\_SZ)  Appid.sys = Driver |
| Computer Configuration > Preferences > Windows Settings > Registry > Replace > HKLM\System\CurrentControlSet\Control\SafeBoot\Network | (REG\_SZ)  discache.sys = Driver |
| Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Accounts: Block Microsoft accounts | Users can't add or log on with Microsoft accounts |
| Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Path Validation Settings > Stores > Allow user trusted root Certificate Authorities (CAs) to be used to validate certificates | Disabled |
| Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Path Validation Settings > Stores > Allow users to trust peer trust certificates | Disabled |
| Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Path Validation Settings > Stores > Root CAs that client computers can trust | Third-Party Root Certification Authorities and Enterprise Root Certification Authorities |
| Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Certificate Path Validation Settings > Stores | CAs must also be compliant with user principal name (UPN) constraints = Disabled |
| Computer Configuration > Administrative Templates >Network > Network Connections > Require domain users to elevate when setting a network's location | Enabled |
| Computer Configuration > Administrative Templates > System > Group Policy > Phone-PC linking on this device | Disabled |
| Computer Configuration > Administrative Templates > System > OS Policies > Allow upload of User Activities | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Allow a shared Books folder | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Allow configuration updates for the Books Library | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Allow extended telemetry for the Books tab | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Antivirus > Turn off Windows Defender Antivirus | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Logon Options > Sign-in last interactive user automatically after a system-initiated restart | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Disable new DMA devices when this computer is locked | Enabled |
| Computer Configuration > Administrative Templates > System > Group Policy > Continue experiences on this device | Disabled |
| Computer Configuration > Administrative Templates > System > Kernel DMA Protection > Enumeration policy for external devices incompatible with Kernel DMA Protection | Enabled:  Enumeration policy: Block all |
| Computer Configuration > Administrative Templates > System > OS Policies > Allow Clipboard History | Disabled |
| Computer Configuration > Administrative Templates > System > OS Policies > Allow Clipboard synchronization across devices | Disabled |
| Computer Configuration > Administrative Templates > System > OS Policies > Allow publishing of User Activities | Disabled |
| Computer Configuration > Administrative Templates > System > OS Policies > Enabled Activity Feed | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Configure collection of browsing data for Microsoft 365 Analytics | Enabled  Configure telemetry collection: Do not allow sending intranet or internet history |
| Computer Configuration > Administrative Templates > Windows Components > Data Collection and Preview Builds > Disable diagnostic data viewer. | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Allow Microsoft Edge to start and load the Start and New Tab page at Windows startup and each time Microsoft Edge is closed | Enabled  Configure tab preloading: Prevent tab preloading |
| Computer Configuration > Administrative Templates > Windows Components > Microsoft Edge > Allow Sideloading of extensions | Disabled |

## Windows Defender configuration

|  |  |
| --- | --- |
| **Group Policy** | **Value(s)** |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Antivirus > MAPS > Configure the ‘Block at First Sight’ feature | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Antivirus > MAPS > Join Microsoft MAPS | Enabled: Advanced |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Antivirus > MAPS > Send file samples when further analysis is required | Enabled: Send safe samples automatically |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Antivirus > Real-time Protection > Turn off real-time protection | Disabled |

## AppLocker configuration

|  |  |
| --- | --- |
| **Group Policy** | **Value(s)** |
| Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Enforcement > Executable Rules | Configured: True Enforce Rules |
| Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Executable Rules | Allow Everyone: All files located in the [Windows Defender\Platform](https://support.microsoft.com/en-us/help/4052623/update-for-windows-defender-antimalware-platform) folder -  %OSDrive%\ProgramData\Microsoft\Windows Defender\Platform\\*  Allow Everyone: All files located in the Program Files folder - with exceptions  Exception: (Path) %PROGRAMFILES%\Windows Kits\\*\Debuggers\\*  Allow Everyone: All files located in the Windows folder - with exceptions  Exception: (Path) %SYSTEM32%\com\dmp\\*  Exception: (Path) %SYSTEM32%\FxsTmp\\*  Exception: (Path) %SYSTEM32%\Spool\drivers\color\\*  Exception: (Path) %SYSTEM32%\Spool\PRINTERS\\*  Exception: (Path) %SYSTEM32%\Spool\SERVERS\\*  Exception: (Path) %SYSTEM32%\Tasks\\*  Exception: (Path) %SYSTEM32%\microsoft\crypto\rsa\machinekeys\\*  Exception: (Path) %WINDIR%\tasks\\*  Exception: (Path) %WINDIR%\temp\\*  Exception: (Path) %WINDIR%\tracing\\*  Exception: (Path) %WINDIR%\registration\crmlog\\*  Exception: (Path) %WINDIR%\servicing\packages\\*  Exception: (Path) %WINDIR%\servicing\sessions\\*  Exception: (Publisher) %SYSTEM32%\WMIC.exe,\*  Exception: (Publisher) %SYSTEM32%\cmstp.exe,\*  Exception: (Publisher) %SYSTEM32%\mshta.exe,\*  Exception: (Publisher) %SYSTEM32%\PresentationHost.exe,\*  Exception: (Publisher) %SYSTEM32%\windbg.exe,\*  Exception: (Publisher) %SYSTEM32%\cipher.exe,\*  Exception: (Publisher) %Microsoft.NET%\Framework64\\*\IEExec.exe  Exception: (Publisher) %Microsoft.NET%\Framework64\\*\InstallUtil.exe  Exception: (Publisher) %Microsoft.NET%\Framework\\*\regsvcs.exe  Exception: (Publisher) %Microsoft.NET%\Framework\\*\msbuild.exe  Exception: (Publisher) %Microsoft.NET%\Framework\\*\regasm.exe  Allow Administrators: All files |
| Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Enforcement > Windows Installer Rules | Configured: True Enforce Rules |
| Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Windows Installer Rules | Allow Administrators: All Windows Installer files  Allow Everyone: (PATH) %WINDIR%\Installer\\* |
| Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Enforcement > Script Rules | Configured: True Enforce Rules |
| Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Script Rules > Enforce rules of this type | Allow Everyone: All Scripts located in the Program Files folder   Allow Everyone: All Scripts located in the Windows folder - with exceptions  Exception: (PATH) %SYSTEM32%\com\dmp\\*  Exception: (PATH) %SYSTEM32%\FxsTmp\\*  Exception: (PATH) %SYSTEM32%\Spool\drivers\color\\*  Exception: (PATH) %SYSTEM32%\Spool\PRINTERS\\*  Exception: (PATH) %SYSTEM32%\Spool\SERVERS\\*  Exception: (PATH) %SYSTEM32%\Tasks\\*  Exception: (PATH) %WINDIR%\registration\crmlog\\*  Exception: (PATH) %WINDIR%\tasks\\*  Exception: (PATH) %WINDIR%\temp\\*  Exception: (PATH) %WINDIR%\tracing\\*  Exception: (PATH) %WINDIR%\servicing\packages\\*  Exception: (PATH) %WINDIR%\servicing\sessions\\*  Exception: (PATH) %SYSTEM32%\microsoft\crypto\rsa\machinekeys\\*  Allow Administrators: All scripts |
| Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Enforcement > DLL Rules | Configured: True Enforce Rules |
| Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > DLL Rules | Allow Everyone: All DLLs located in the [Windows Defender\Platform](https://support.microsoft.com/en-us/help/4052623/update-for-windows-defender-antimalware-platform) folder -  %OSDrive%\ProgramData\Microsoft\Windows Defender\Platform\\*  Allow Everyone: All DLLs located in the Program Files folder  Allow Everyone: All DLLs located in the Windows folder - with exceptions  Exception: (PATH) %SYSTEM32%\com\dmp\\*  Exception: (PATH) %SYSTEM32%\FxsTmp\\*  Exception: (PATH) %SYSTEM32%\Spool\drivers\color\\*  Exception: (PATH) %SYSTEM32%\Spool\PRINTERS\\*  Exception: (PATH) %SYSTEM32%\Spool\SERVERS\\*  Exception: (PATH) %SYSTEM32%\Tasks\\*  Exception: (PATH) %SYSTEM32%\microsoft\crypto\rsa\machinekeys\\*  Exception: (PATH) %WINDIR%\registration\crmlog\\*  Exception: (PATH) %WINDIR%\tasks\\*  Exception: (PATH) %WINDIR%\temp\\*  Exception: (PATH) %WINDIR%\tracing\\*  Exception: (PATH) %WINDIR%\servicing\packages\\*  Exception: (PATH) %WINDIR%\servicing\sessions\\*  Allow Administrators: All DLLs |
| Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Enforcement > Packaged app Rules | Configured: True Enforce Rules |
| Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Packaged app rules | Allow Everyone: All signed packaged apps  Exception: (Publisher) Microsoft.Getstarted  Exception: (Publisher) Microsoft.MicrosoftOfficeHub  Exception: (Publisher) Microsoft.SkypeApp  Exception: (Publisher) Microsoft.WindowsFeedback |

## BitLocker configuration

|  |  |
| --- | --- |
| **Group Policy** | **Value(s)** |
| Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Enforce drive encryption type on operating system drives | Enabled  Select the encryption type: Full encryption |
| Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Configure use of hardware-based encryption for operating system drives | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives > Require additional authentication at startup | Enabled  Allow BitLocker without a compatible TPM (Requires a password or startup key on a USB flash drive): Unticked  Configure TPM startup: Do not allow TPM  Configure TPM startup PIN: Allow startup PIN with TPM  Configure TPM startup key: Do not allow startup key with TPM  Configure TPM startup key and PIN: Allow startup key and PIN with TPM |

|  |
| --- |
| **Group Policy > Computer Configuration > Administrative Templates > Windows Components > Operating System Drives** |
| Allow enhanced PINs for startup |
| Configure minimum PIN length for startup |
| Configure use of passwords for operating system drives |

## Windows Defender Exploit Guard configuration

|  |  |
| --- | --- |
| **Group Policy** | **Value(s)** |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Antivirus > Windows Defender Exploit Guard > Controlled folder access | Enabled  Mode: Block |
| Computer Configuration > Administrative Templates > Windows Components > Window Defender Exploit Guard> Use a common set of exploit protection settings | Enabled.  A *UNC path to an XML file containing any desired settings should be configure*d. |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Antivirus > Windows Defender Exploit Guard > Attack Surface Reduction > Configure Attack Surface Reduction rules  *Details on these policies can be found at*[*https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard*](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard) | d4f940ab-401b-4efc-aadc-ad5f3c50688a: 1  9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2: 1  3b576869-a4ec-4529-8536-b80a7769e899: 1  5beb7efe-fd9a-4556-801d-275e5ffc04cc: 1  92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B: 1  b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4: 1  75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84: 1  d3e037e1-3eb8-44c8-a917-57927947596d: 1  be9ba2d9-53ea-4cdc-84e5-9b1eeee46550: 1  26190899-1602-49e8-8b27-eb1d0a1ce869: 1  7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c: 1  d1e49aac-8f56-4280-b9ba-993a6d77406c: 2 |

## Windows Defender Device Guard and Application Control configuration

|  |  |
| --- | --- |
| **Group Policy** | **Value(s)** |
| Computer Configuration > Administrative Templates > System > Device Guard > Turn On Virtualisation Based Security | Enabled:  Platform Security: Secure Boot and DMA Protection  Virtualization Based Protection of Code Integrity: Enabled with UEFI Lock  Require UEFI Memory Attributes Table: Enabled\*  Credential Guard Configuration:  Enabled with UEFI Lock  Secure Launch Configuration: Enabled |

## Windows Defender Application Guard configuration

|  |  |
| --- | --- |
| **Group Policy** | **Value(s)** |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Turn on Windows Defender Application Guard in Enterprise Mode | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Allow data persistence for Windows Defender Application Guard | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Allow auditing events in Windows Defender Application Guard | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Prevent enterprise websites from loading non-enterprise content | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Configure Windows Defender Application Guard clipboard settings | Enabled:  Enable clipboard operation from an isolated session to the host. Clipboard content options: 3 (Allow text and image copying) |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Configure Windows Defender Application Guard print settings | Enabled:  Allowed Print types in Application Guard: 11 (Allow network, PDF and XPS printing) |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Allow files to download and save to the host operating system from Windows Defender Application Guard | Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Configure additional sources for untrusted files in Windows Defender Application Guard | Enabled:  Removable media: Enabled  Network shares: Enabled  Files with Mark of the Web: Enabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Allow Windows Defender Application Guard to use Root Certificate Authorities from the user’s device | Disabled |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Allow users to trust files that open in Windows Defender Application Guard | Enabled:  0. Do not allow users to manually trust files |
| Computer Configuration > Administrative Templates > Windows Components > Windows Defender Application Guard > Allow camera and microphone access in Windows Defender Application Guard | Disabled |
| Computer Configuration  > Administrative Templates > Network > Network Isolation > Enterprise resource domains hosted in the cloud | Enabled:  *Any trusted websites that should not load in Application Guard. To allow any subdomain of a given domain.* |
| Computer Configuration  > Administrative Templates > Network > Network Isolation > Private network ranges for apps | Enabled:  Any IP address ranges that are used for internal applications. These can be specified in CIDR notation. |

## Windows Defender Firewall configuration

|  |  |
| --- | --- |
| **Group Policy** | **Value(s)** |
| Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Domain Profile | Firewall State : On (Recommended)  Inbound connections : Block (default)  Outbound connections : Allow (default) |
| Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Domain Profile > Settings > Customize > Apply local firewall rules | No |
| Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Private Profile | Firewall State : On (Recommended)  Inbound connections : Block (default)  Outbound connections : Block |
| Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Private Profile > Settings > Customize > Apply local firewall rules | No |
| Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Public Profile | Firewall State : On (Recommended)  Inbound connections : Block (default)  Outbound connections : Block |
| Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall Properties > Public Profile > Settings > Customize > Apply local firewall rules | No |
| Computer Configuration > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Outbound Rules | Enabled  Allow outbound DHCP  General > Action: Allow the connection  Programs and Services > Programs > This Program > %SystemRoot%\system32\svchost.exe  Allow Programs and Services > Service > Apply to this service > DHCP Client (Dhcp)  Advanced > Profiles: Private, Public  Protocols and Ports > Local port: UDP 68  Protocols and Ports > Remote port: UDP 67  Allow outbound DNS  General > Action: Allow the connection  Programs and Services > Programs > This Program > %SystemRoot%\system32\svchost.exe  Allow Programs and Services > Service > Apply to this service > DNS Client (Dnscache)  Advanced > Profiles: Private, Public  Protocols and Ports > Remote port: TCP 53, UDP 53  Allow outbound Kerberos  General > Action: Allow the connection  Programs and Services > Programs > This Program > %SystemRoot%\system32\lsass.exe  Advanced > Profiles: Private, Public  Protocols and Ports > Remote port: All TCP and UDP ports  Allow outbound LDAP  General > Action: Allow the connection  Programs and Services > Programs > This Program > All programs that meet the specified conditions  Advanced > Profiles: Private, Public  Protocols and Ports > Remote port: TCP 389, UDP 389  General > Action: Allow the connection  Programs and Services > Programs > This Program > %SystemRoot%\system32\svchost.exe  Allow Programs and Services > Service > Apply to this service > Network Location Awareness (NlaSvc)  Advanced > Profiles: Private, Public  Protocols and Ports > Remote port: TCP 80 |

## VPN configuration

|  |  |
| --- | --- |
| **IKEv2** | **Selection** |
| Encryption | AES with 128-bit keys in GCM-128 mode |
| Pseudo-Random Function | HMAC-SHA-256 (RFC4868) |
| Diffie-Hellman Group | Group 19 256-bit random ECP (RFC5903) |
| Authentication | X.509 certificates with ECDSA signatures (256-bit) on the P-256 curve and SHA-256 (RFC4945 and RFC4055) |
| **ESP** | **Selection** |
| Encryption | AES with 128-bit keys in CBC mode (RFC3602) |
| Integrity | SHA-256 (RFC4846) |

## Management of UEFI firmware settings

|  |  |
| --- | --- |
| **Setting** | **Value** |
| Administrator/Setup Password + UEFI Lockout | A UEFI administrator or setup password should be set and UEFI console lockout enabled to prevent unauthourised changes to UEFI settings. |
| Boot Mode | UEFI |
| Secure Boot | Enabled |
| Legacy Boot Options and Legacy Option ROMs | Disabled |
| Manufacturer Signed Firmware Updates | Enabled |
| Trusted Platform Module (TPM) | Enabled |
| UEFI Firmware Rollback | Disabled |
| Boot Options | Restricted to only those that are required. Priority should be given to internal storage. |
| Boot Order | Locked |
| No Execute (NX) | Enabled |
| Virtualisation Extensions | Enabled |
| Input/Output Memory Management Unit (IOMMU) | Enabled |
| Thunderbolt | Ports should be disabled if not required  If required  ·              Disable Thunderbolt boot support if not required.  ·              Disable Thunderbolt pre-boot module support.  ·              Set a minimum Thunderbolt Security Level of User Authorisation. |

## Windows 10 Enterprise feature updates

|  |  |
| --- | --- |
| **Group Policy** | **Value(s)** |
| Computer Configuration  > Administrative Templates > Windows Components > Windows Update > Remove access to “Pause updates” feature | Enabled |
| Computer Configuration  > Administrative Templates > Windows Components> Windows Update > Windows Update for Business > Manage preview builds | Disabled |
| Computer Configuration  > Administrative Templates > Windows Components > Windows Update > Windows Update for Business > Select when Preview Builds and Feature Updates are received | Select the Windows readiness level for the updates you want to receive: Semi-Annual Channel  After a Preview Build or Feature Update is released, defer receiving it for this many days: 0 |

# Standard Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Standard can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Standard. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Review the operating system configuration settings | * Confirm from the standard if the configuration settings on the operating system are the same |

## Enforcement

All staff of XXXX must comply with all Information Security Standards. Failure to comply with these standards may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Standard statements described in this document must be reviewed and approved in accordance with the Exception Process defined in *XXXX-POL-ALL-001 - Information Security Policy Framework*

## Glossary / Acronyms

|  |  |
| --- | --- |
| UEFI | Unified Extensible Firmware Interface |
| ROM | Read Only Memory |
| AES | Advanced Encryption Standard |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| DHCP | Dynamic Host Configuration Protocol |
| CIDR | Classless Inter Domain Routing |
| DMA | Direct Memory Access |
| TPM | Trusted Platform Module |
| DLL | Dynamic Link Library |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |

## Document Ownership

This Standard is owned by the YYYY

## Document Coordinator

This Standard is coordinated by the YYYY

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Distribution

* *Information Security*
* *IT Department*