Windows 7 Logo Program

Qualification requirements for products that run on the Microsoft® Windows® 7 operating system

Technical Requirements for the Windows 7 Software Logo Program for Client Operating Systems

This document outlines the proposed requirements for the Windows Logo Program for Windows 7. Feedback on these requirements can be submitted online at: <http://go.microsoft.com/?linkid=9630188>

**Microsoft Confidential. ©** 2007 Microsoft Corporation. All rights reserved. These materials are confidential to and maintained as a trade secret by Microsoft Corporation. Information in these materials is restricted to Microsoft authorized recipients only. Any use, distribution or public discussion of, and any feedback to, these materials is subject to the terms of the attached license. By providing any feedback on these materials to Microsoft, you agree to the terms of that license.

**Microsoft Corporation Technical Documentation License Agreement (Standard)**
**READ THIS!** THIS IS A LEGAL AGREEMENT BETWEEN MICROSOFT CORPORATION ("MICROSOFT") AND THE RECIPIENT OF THESE MATERIALS, WHETHER AN INDIVIDUAL OR AN ENTITY ("YOU"). IF YOU HAVE ACCESSED THIS AGREEMENT IN THE PROCESS OF DOWNLOADING MATERIALS ("MATERIALS") FROM A MICROSOFT WEB SITE, BY CLICKING "I ACCEPT", DOWNLOADING, USING OR PROVIDING FEEDBACK ON THE MATERIALS, YOU AGREE TO THESE TERMS. IF THIS AGREEMENT IS ATTACHED TO MATERIALS, BY ACCESSING, USING OR PROVIDING FEEDBACK ON THE ATTACHED MATERIALS, YOU AGREE TO THESE TERMS.

1. For good and valuable consideration, the receipt and sufficiency of which are acknowledged, You and Microsoft agree as follows:

(a) If You are an authorized representative of the corporation or other entity designated below ("**Company**"), and such Company has executed a Microsoft Corporation Non-Disclosure Agreement that is not limited to a specific subject matter or event ("**Microsoft NDA**"), You represent that You have authority to act on behalf of Company and agree that the Confidential Information, as defined in the Microsoft NDA, is subject to the terms and conditions of the Microsoft NDA and that Company will treat the Confidential Information accordingly;

(b) If You are an individual, and have executed a Microsoft NDA, You agree that the Confidential Information, as defined in the Microsoft NDA, is subject to the terms and conditions of the Microsoft NDA and that You will treat the Confidential Information accordingly; or

(c)If a Microsoft NDA has not been executed, You (if You are an individual), or Company (if You are an authorized representative of Company), as applicable, agrees: (a) to refrain from disclosing or distributing the Confidential Information to any third party for five (5) years from the date of disclosure of the Confidential Information by Microsoft to Company/You; (b) to refrain from reproducing or summarizing the Confidential Information; and (c) to take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, but no less than reasonable care, to keep confidential the Confidential Information. You/Company, however, may disclose Confidential Information in accordance with a judicial or other governmental order, provided You/Company either (i) gives Microsoft reasonable notice prior to such disclosure and to allow Microsoft a reasonable opportunity to seek a protective order or equivalent, or (ii) obtains written assurance from the applicable judicial or governmental entity that it will afford the Confidential Information the highest level of protection afforded under applicable law or regulation. Confidential Information shall not include any information, however designated, that: (i) is or subsequently becomes publicly available without Your/Company’s breach of any obligation owed to Microsoft; (ii) became known to You/Company prior to Microsoft’s disclosure of such information to You/Company pursuant to the terms of this Agreement; (iii) became known to You/Company from a source other than Microsoft other than by the breach of an obligation of confidentiality owed to Microsoft; or (iv) is independently developed by You/Company. For purposes of this paragraph, "Confidential Information" means nonpublic information that Microsoft designates as being confidential or which, under the circumstances surrounding disclosure ought to be treated as confidential by Recipient. "Confidential Information" includes, without limitation, information in tangible or intangible form relating to and/or including released or unreleased Microsoft software or hardware products, the marketing or promotion of any Microsoft product, Microsoft's business policies or practices, and information received from others that Microsoft is obligated to treat as confidential.

2. You may review these Materials only (a) as a reference to assist You in planning and designing Your product, service or technology ("Product") to interface with a Microsoft Product as described in these Materials; and (b) to provide feedback on these Materials to Microsoft. All other rights are retained by Microsoft; this agreement does not give You rights under any Microsoft patents. You may not (i) duplicate any part of these Materials, (ii) remove this agreement or any notices from these Materials, or (iii) give any part of these Materials, or assign or otherwise provide Your rights under this agreement, to anyone else.

3. These Materials may contain preliminary information or inaccuracies, and may not correctly represent any associated Microsoft Product as commercially released. All Materials are provided entirely "AS IS." To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

4. If You are an entity and (a) merge into another entity or (b) a controlling ownership interest in You changes, Your right to use these Materials automatically terminates and You must destroy them.

5. You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to these Materials. However, any Feedback you voluntarily provide may be used in Microsoft Products and related specifications or other documentation (collectively, "Microsoft Offerings") which in turn may be relied upon by other third parties to develop their own Products. Accordingly, if You do give Microsoft Feedback on any version of these Materials or the Microsoft Offerings to which they apply, You agree: (a) Microsoft may freely use, reproduce, license, distribute, and otherwise commercialize Your Feedback in any Microsoft Offering; (b) You also grant third parties, without charge, only those patent rights necessary to enable other Products to use or interface with any specific parts of a Microsoft Product that incorporate Your Feedback; and (c) You will not give Microsoft any Feedback (i) that You have reason to believe is subject to any patent, copyright or other intellectual property claim or right of any third party; or (ii) subject to license terms which seek to require any Microsoft Offering incorporating or derived from such Feedback, or other Microsoft intellectual property, to be licensed to or otherwise shared with any third party.

6. Microsoft has no obligation to maintain confidentiality of any Microsoft Offering, but otherwise the confidentiality of Your Feedback, including Your identity as the source of such Feedback, is governed by Your NDA.

7. This agreement is governed by the laws of the State of Washington. Any dispute involving it must be brought in the federal or state superior courts located in King County, Washington, and You waive any defenses allowing the dispute to be litigated elsewhere. If there is litigation, the losing party must pay the other party’s reasonable attorneys’ fees, costs and other expenses. If any part of this agreement is unenforceable, it will be considered modified to the extent necessary to make it enforceable, and the remainder shall continue in effect. This agreement is the entire agreement between You and Microsoft concerning these Materials; it may be changed only by a written document signed by both You and Microsoft.



**Introduction**

The purpose of this document is to outline the proposed technical requirements that an application must meet in order to participate in the Windows 7 Software Logo Program.

**Program Overview**

Windows has a broad ecosystem of products and partners that all support Windows. Displaying the Windows brand on your product represents a relationship and a shared commitment to quality between Microsoft and your company. Customers trust that seeing the Windows brand on your product ensures that it has been verified to work well on Windows.

The Windows 7 Software Logo program is made up of policies and requirements that help ensure logo’d applications are easy to install and reliable on PCs running Windows 7.

**To obtain the logo the partner must:**

1. Include business and technical owners for all submissions
2. Opt in to receive communications from Microsoft about their products
3. Include a copy and license of the software for compatibility testing purposes
4. Along with Microsoft agree to a 30-90 day resolution policy for all issues identified in market with logo’d products
5. Ensure the application adheres to all policies and passes all requirements in this document

**Policies**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
|  |  |

**Num.** |

|  |  |
| --- | --- |
| **TitleUse SHIFT+ENTER to open the menu (new window).****http://appx/_layouts/images/blank.gifhttp://appx/_layouts/images/blank.gif** | **http://appx/_layouts/images/blank.gif** |

 | **RationaleFilter** | **CriteriaFilter** |
| Policy 1 |

|  |  |
| --- | --- |
| Comply with Anti-spyware Coalition GuidelinesUse SHIFT+ENTER to open the menu (new window). |  |

 | Malware is a major concern for customers.  When they buy software that carries the Windows logo, they need to know that it is free of malware. | Microsoft does not logo Malware or Spyware. Any application found to be Malware or Spyware as defined by the Anti-Spyware Coalition will lose their logo status and any related benefits. Definition:Spyware (and other potentially unwanted technologies) Technologies deployed without appropriate user consent and/or implemented in ways that impair user control over: 1. Material changes that affect their user experience, privacy, or system security
2. Use of their system resources, including what programs are installed on their computers; and/or
3. Collection, use, and distribution of their personal or other sensitive information.
 |
| Policy 2 |

|  |  |
| --- | --- |
| Do not modify WRP protected resourcesUse SHIFT+ENTER to open the menu (new window). | http://appx/_layouts/images/blank.gif |

 | Windows Resource Protection (WRP) is designed to ensure that protected system resources are updated only by using Microsoft-approved installation or update mechanisms.  Following WRP guidelines will help improve system reliability. | Applications must not attempt to install files or modify registry keys that are protected by Windows Resource Protection (WRP). If the application requires newer versions of system components, it must update these components by using a Microsoft Service Pack or Microsoft-approved installation package containing the system component.  System components must never be repackaged. |
| Policy 3 |

|  |  |
| --- | --- |
| Ensure ongoing quality |  |

 | Having your product logo'd represent a relationship between you and Microsoft. | 1. ISVs must sign up to receive their crash data from Windows Error Reporting. This can be accomplished by signing up at: [https://winqual.microsoft.com](https://winqual.microsoft.com/).  ISVs must map their logo'd applications to their company at this site and maintain those mappings while the product is supported.
2. If an application with the Windows Logo is found in the top 20% of all reported crashes, the application must be fixed within 90 days.
3. If an issue is reported with a logo’d product that turns out to be in violation of the logo requirements, Microsoft will confirm the issue and reach out to the partner for resolution.
4. Microsoft will alert partners if through compatibility testing with OS updates or future OS versions, if an issue is identified with the product.
 |

**Requirements**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |
| --- | --- |
|  |  |

**Num.** |

|  |  |
| --- | --- |
| **TitleUse SHIFT+ENTER to open the menu (new window).****http://appx/_layouts/images/blank.gifhttp://appx/_layouts/images/blank.gif** | **http://appx/_layouts/images/blank.gif** |

 | **RationaleFilter** | **CriteriaFilter** |
| 1 |

|  |  |
| --- | --- |
| Install and uninstall cleanlyUse SHIFT+ENTER to open the menu (new window). | http://appx/_layouts/images/blank.gif |

 | Clean, reversible, installation allow users to successfully manage (deploy, inventory, remove) their applications. **CREATE REGISTRY ENTRIES**Inventory tools require accurate and complete information about installed applications.  Applications must create the correct registry settings to allow successful detection and successful uninstalls.   | Applications must properly implement a clean, reversible, installation. **Installation Requirements**An application installation should never:1. Force immediate reboot, i.e.: a reboot should never be the only option at the end of an install.  Users should have the opportunity to restart later.
2. Use 8.3 SFN “short file names”

The following registry entries must be created at installation:1. DisplayName
2. InstallLocation
3. Publisher
4. UninstallString
5. VersionMajor or MajorVersion
6. VersionMinor or MinorVersion
 |
| 2 |

|  |  |
| --- | --- |
| Install to the correct folders by defaultUse SHIFT+ENTER to open the menu (new window). | http://appx/_layouts/images/blank.gif |

 | Users should have a consistent and secure experience with the default installation location of files, while maintaining the option to install an application to the location they choose. It is also important to store application data in the correct location to allow several people to use the same computer without corrupting or overwriting each other's data and settings. | Applications should be installed to the "**Program Files**" folder by default. 1. **Per-machine Installations**The per-machine installations of an application means that the application is available for all users of a computer. Please note that in the Per- machine installations, user data must be written at first run and not during the installation as there is no correct user location to store date at time of installation.
	* 1. For “per machine” installations, user data must be written at first run and not during the installation.
		2. Since the install potentially elevates to a different user account during a “per machine” install, there is no correct user location to store date at time of installation.
2. **Per-user Installations**The per-user installation of an application means that the application is available only for a particular user. In Per User installation Determine the type of application data you are storing in the file system. Is it computer-dependent, computer-independent, or low-rights integrity data? Based on that information, use one of the following paths to store the data:
	1. **Appdata\Local**
		1. For Per-user ***computer-dependent***application data. Should not be roamed or redirected within an organization.
		2. Application data that contains only temporary or non-critical data that can be discarded without affecting the application's functionality. (For example, log files for debugging purposes.
		3. Application data which, although machine independent, can easily be re-created without explicit user action, as it does not store any user-generated customizations or settings.
	2. **Appdata\LocalLow**
		1. For per-user ***low-rights application data***. Meant as a location to be used by low-rights
		2. Applications to store their data. Will not be roamed or redirected in an organization.
	3. **AppData\Roaming**
		1. For per-user ***computer-independent*** application data. Can be roamed or redirected within an organization by using folder redirection or roaming user profiles.

Computer-independent application data that contains a user's customizations and cannot be recreated without explicit user action. |
| 3 |

|  |  |
| --- | --- |
| Support x64 versions of WindowsUse SHIFT+ENTER to open the menu (new window). | http://appx/_layouts/images/blank.gif |

 | As x64 hardware becomes more prevalent, users expect applications to run on x64 platforms.  | To maintain compatibility with 64bit versions of Windows, it is necessary that:1. Applications and their installers must not contain any 16-bit code or rely on any 16-bit component
2. The application setup must detect and install the proper drivers and components for the 64-bit architecture
3. Any shell plugins must run on 64-bit versions of Windows
4. Applications running under wow64 must not run their own wow64 detection checks or redirects, the OS must manage such activities
 |
| 4 |

|  |  |
| --- | --- |
| Follow User Account Control (UAC) GuidelinesUse SHIFT+ENTER to open the menu (new window). | http://appx/_layouts/images/blank.gif |

 | Following UAC guidelines provides applications with the necessary permissions when needed, without leaving the system constantly exposed to security risks. | Applications must have an embedded manifest that defines its execution level:1. <requestedExecutionLevel level="asInvoker | highestAvailable | requireAdministrator" uiAccess="true|false"/>
2. The main process of the application must be run as a standard user (asInvoker).  Any administrative features must be moved into a separate process that runs with administrative privileges.

A UAC waiver is required for:1. Applications that run their main process with elevated privileges (requireAdministrator or highestAvailable).

Waivers will be considered for the following scenarios:1. Applications that need to drive input to the UI of another window (may set uiAccess=true).
2. Administrative system tools
3. NT Services that have no user interaction

Note:  Additional UAC guidance can be found at: <http://msdn.microsoft.com/en-us/library/aa905330.aspx> |
| 5 |

|  |  |
| --- | --- |
| Do not load Services and Drivers in Safe ModeUse SHIFT+ENTER to open the menu (new window). | http://appx/_layouts/images/blank.gif |

 | Safe Mode is designed to allow users to diagnose and trouble-shoot Windows. Unless needed for basic operations of the system (for example, storage device drivers) or for diagnostic and recovery purposes (for example, anti-virus scanners), drivers and services must not be set to load in safe mode. | By default, most drivers and services that did not come preinstalled with Windows are not started in Safe Mode.  They should remain disabled unless they are needed for basic operations of the system or for diagnostic and recovery purposes. Drivers and services that must be started in Safe Mode require a waiver.  Each applicable driver or service must be listed in the waiver.  The application installer must register all such drivers and services using these registry keys:1. HKLM/System/CurrentControlSet/Control/SafeBoot/Minimal
2. HKLM/System/CurrentControlSet/Control/SafeBoot/Network

These drivers and services must also be tested to ensure that they function in Safe Mode without any errors. |
| 6 |

|  |  |
| --- | --- |
| Digitally Sign FilesUse SHIFT+ENTER to open the menu (new window). | http://appx/_layouts/images/blank.gif |

 | Digital signatures allow the administrator or end-user who is installing Windows-based software to know whether a legitimate publisher has provided the software package. Code Integrity is a Windows feature that improves the security of the operating system by verifying the integrity of a file each time the image of the file is loaded into memory. It detects if a system binary file has been modified by malicious code.   | All executable files must be signed with an Authenticode certificate.  Examples includes files with the following extensions: exe, dll, ocx, sys, cpl, drv, scr.  More information at: <http://msdn.microsoft.com/en-us/library/ms995347.aspx> All kernel mode drivers that are installed by the application must have a Microsoft signature obtained through the WHQL or DRS program.  Detailed information is available at: <http://www.microsoft.com/whdc/winlogo/drvsign/kmsigning.mspx> Waivers are available for 3rd party redistributables when requests for signed version have not been successful. |
| 7 |

|  |  |
| --- | --- |
| Do not prevent an installation or application from launching because of OS version checkingUse SHIFT+ENTER to open the menu (new window). | http://appx/_layouts/images/blank.gif |

 | It is important that customers are not artificially prevented from installing or running their applications when there are no technical limitations.    | Applications should have no reason to check the O/S version in general, if necessary version checks should be done only by the installer, and not the installed application, or driver.Waivers will be granted for applications meeting the criteria below:1. Applications that check only the minimum version of the OS (during install only, not at runtime) by using only the approved API calls, and properly listing the minimum version requirement in the application manifest
2. Security applications (antivirus, firewall, etc), system utilities – defrag, backups, and diagnostics tools that check the OS version by using only the approved API calls
3. Applications that are delivered as one package that runs on Windows XP, Windows Vista, and Windows 7, and needs to check the O/S version to determine which components to install on a given operating system.
 |
| 8 |

|  |  |
| --- | --- |
| Prevent unnecessary rebootsUse SHIFT+ENTER to open the menu (new window). | http://appx/_layouts/images/blank.gif |

 | The primary reason software updates require a system restart during an installation or update is that some of the files that are being updated are currently being used by a running application or service. The Restart Manager enables all but the critical system services to be shut down and restarted. This frees files that are in use and allows installation operations to complete. System reboots are a major disruption and lead to a bad user experience.  By 1. registering for a restart when needed, and 2. listening for shutdown messages, applications can reduce system reboots during installations and updates.More information is available at:[http://msdn.microsoft.com/en-us/library/aa373651(VS.85).aspx](http://msdn.microsoft.com/en-us/library/aa373651%28VS.85%29.aspx) | Application installation must take advantage of the Restart Manager APIs to perform system reboots. While running application must be restart manager aware and listen and respond to the following shutdown messages:1. WM\_QUERYENDSESSION with LPARAM = ENDSESSION\_CLOSEAPP(0x1): GUI applications must respond (TRUE) immediately in preparation for a restart
2. WM\_ENDSESSION with LPARAM = ENDSESSION\_CLOSEAPP(0x1): Applications must return a 0 value within 30 seconds and shutdown
3. CTRL C:  Console applications that receive this message should shutdown immediatelyDrivers must not veto a system shutdown event

Upon receiving a system shutdown message, applications that have unsaved user data must prompt the user to save their data. |
| 9 |

|  |  |
| --- | --- |
| Support multiuser sessionsUse SHIFT+ENTER to open the menu (new window). | http://appx/_layouts/images/blank.gif |

 | Windows users should be able to run concurrent sessions without conflict or disruption. Applications must ensure that when running in multiple sessions either locally or remotely, the normal functionality of the application should not be impacted. Application settings and data files should not be persisted across users. A user’s privacy and preferences should be isolated to the user’s session. | 1. User applications must be able to run in multiple user sessions (Fast User Switching) for both local and remote access. If an application doesn’t allow for multiple sessions a waiver is needed. If an application does not support multiple user sessions or remote access, it must clearly state this when launched from such a session and write a message to the application event log.  Applications must check other TS sessions for existing instances of the application.
2. Application instances must be isolated from each other. This means that user data from one instance is not visible to another application instance.  Sound in an inactive user session should not be heard in an active user session. When multiple application instances use shared resources, the application must make sure that there is not a conflict.
3. If an application is installed for multiple users, data needs to be written to the correct file and registry locations. As in the UAC requirement, it is necessary that user data is written on first run and not at install.
 |
| 10 | Minimize application failures | Application failures such as crashes and hangs are top drivers of customer dissatisfaction. Eliminating such failures improves application stability/responsiveness and reduces loss of time, work, data, and control for the user. | Any errors found in the following Application Verifier tests must be fixed:1. Basics: Exceptions, Handles, Heaps, Locks, Memory, TLS
2. Miscellaneous:  DangerousAPIs, DirtyStacks

Windows Error Reporting must not be disabled.  If a fault (such as an Access Violation) is injected into an application, the application must allow Windows Error Reporting to report this crash |

Feedback on these requirements can be submitted online at: <http://go.microsoft.com/?linkid=9630188>