

Steve Sisolak
Governor



Laura E. Freed
Director

Colleen Murphy
Deputy Director

Alan Cunningham
State Chief Information Officer

STATE OF NEVADA
DEPARTMENT OF ADMINISTRATION

Enterprise IT Services Division

100 N. Stewart Street, Suite 100 | Carson City, Nevada 89701

Phone: (775) 684-5800 | www.it.nv.gov | Fax: (775) 687-9097

MEMORANDUM

December 8, 2020

TO: All Agencies

FROM: Alan Cunningham, State CIO
Department of Administration
Enterprise IT Services Division

SUBJECT: **Final Decommissioning of MS Windows 7 Devices from the State Network**

Per the attached memorandum, issued September 20, 2019, agencies have had 26 months to remove and/or replace the now unsupported and defunct Microsoft operating system WINDOWS 7. Agencies should have taken all necessary steps to either upgrade, replace, or remove all such devices from the network. **The final deadline for WINDOWS 7 device removal is December 31, 2020.**

During the past 26 months, the State Chief Security Information Officer (CISO), Robert Dehnhardt, worked closely with assigned agency Information Security Officers (ISOs) to assist and instruct regarding the decommissioning process. As previously notified, and in accordance with State Security Standards S.2.05.02 and S.5.07.01, any device found connected to the state network using MS WINDOWS 7 must be removed from the network. Please note that this includes devices that were previously patched with a WINDOWS 7 extended Microsoft support license.

Agency ISOs received prior information and instruction to help agencies address the situation. Previous steps and notifications regarding decommissioning of WINDOWS 7 included:

- Microsoft official announcements,
- Notifications to agencies/agency ISOs regarding WINDOWS 7 decommissioning,
- Provision of Extended Microsoft Support Licenses for WINDOWS 7 for interim support,
- Distribution of updated WINDOWS 7 device lists by agency,
- Review, instruction, and discussion during monthly State Information Security Committee (SISC) meetings regarding the decommissioning of WINDOWS 7,
- Ongoing SilverNet scans and agency internal network scanning services to identify offending devices, and

- Ongoing offers of WINDOWS 7 evaluation, planning, and support to agency ISOs regarding the decommissioning process.

After December 31, 2020, agencies will bear all security breach impacts, potential business or application disruptions, and related costs that may occur if current WINDOWS 7 devices are not properly decommissioned and removed from the network. Incurring a cyber security breach from any defunct WINDOWS 7 device on any state network will have far-reaching impact to the state.

Questions or comments regarding the above should be addressed to the State CISO:

Bob Dehnhardt, State Chief Information Security Officer

State of Nevada Department of Administration, Office of Information Security

(775) 684-7322

rwdehnhardt@admin.nv.gov

Agencies must take necessary steps to either upgrade, replace, or remove all WINDOWS 7 devices from the network by the final deadline: December 31, 2020.

WINDOWS 7 - Agency Decommissioning Status

Agency	WIN 7 Count as of 12/04/20	... as of 10/02/20	... as of 9/25/20	... as of 9/18/20	... as of 9/11/20	... as of 8/28/20
Administration	20	23	22	23	24	28
Agriculture	5	6	6	7	7	7
Boards & Commissions						
Board of Nursing	3	3	3	3	3	3
Massage Therapy	0	0	0	0	0	0
Medical Examiners	0	0	0	0	0	0
Occupational Therapists	0	0	0	0	0	0
Public Utilities Commission	12	13	14	14	14	13
Business and Industry	6	9	9	9	8	11
Charter Schools	0	0	0	0	0	0
Conservation and Natural Resources	6	8	10	10	11	10
Controller's Office	1	2	2	2	2	2
Corrections	0	0	0	0	0	0
Economic Development	4	6	6	6	6	5
Education	44	42	42	39	43	50
Employment, Training and Rehabilitation	33	33	34	36	37	37
Health & Human Services						
Aging and Disability Services	0	0	0	0	0	0
Child and Family Services	3	3	3	4	4	3
Healthcare Finance and Policy	0	0	0	0	0	0
Public and Behavioral Health	2	2	2	2	3	3
Welfare	2	5	5	6	6	5
Motor Vehicles	89	93	95	95	95	95
PEBP	0	0	0	0	0	0
Public Safety	3	7	8	12	14	13
Secretary of State	0	0	0	0	0	0
Health Insurance Exchange	1	2	2	2	2	2
Taxation	69	122	122	123	125	181
Tourism and Cultural Affairs	19	30	31	33	35	37
Transportation	3	7	7	5	5	7
Treasurer's Office	0	0	0	0	0	0
Veterans Services	0	1	1	2	2	3
Wildlife	0	1	2	2	2	2
TOTALS	325	418	426	435	448	517

Gray = no WIN7 devices registering on SilverNet

Steve Sisolak
Governor



Deonne E. Contine
Director

Robin Hager
Deputy Director

Michael Dietrich
State Chief Information Officer

David Haws
Administrator

STATE OF NEVADA
DEPARTMENT OF ADMINISTRATION


Enterprise IT Services Division

100 N. Stewart Street, Suite 100 | Carson City, Nevada 89701

Phone: (775) 684-5800 | it.nv.gov | Fax: (775) 687-9097

MEMORANDUM

TO: Department Directors
Division Administrators

FROM: Bob Dehnhardt, State Chief Information Security Officer 

DATE: September 20, 2019

SUBJECT: Windows 7 and Server 2008R2 End-Of-Life

Windows 7 and Windows Server 2008r2 will go out of support on January 14, 2020. This means Microsoft will no longer supply any public security patches for these operating systems after that date, and any vulnerabilities that exist on that date will continue to exist unpatched into the future. If history is any indicator, malicious hackers are now hoarding any Windows 7 or Server 2008r2 vulnerabilities they find and readying them for use on January 15, 2020.

The use of any unsupported software on Silvernet is a significant risk to the State, which is why such use is prohibited under State Security Standard S.5.07.01 – IT Operating System Patch Upgrade Management – which states “Operating Systems, service packs or commercial applications that have reached end-of-support from the vendor must be upgraded to a currently supported version.” (Section 6.0.E)

This issue was first raised to agency Information Security Officers in September 2018 and has been mentioned or discussed at every State Information Security Committee meeting since January 2019. At this point, all agencies should be well on their way to completing the migration to Windows 10, but a September 18, 2019 report shows that there are over 5,000 systems still running Windows 7 on the State networks.

The preferred way to address this is to upgrade all Windows 7 systems to Windows 10 before January 2020. The per-system cost for these upgrade licenses is \$123, available through EITS in our Enterprise license agreement with Microsoft. However, there may be systems that may not be able to effectively run Windows 10 and are not currently budgeted for replacement, or there may be resource or other constraints that will prevent the upgrades from happening before January 2020. Agencies that feel they may not meet the January 14, 2020 deadline for migrating to Windows 10 should have alternate plans under consideration. At present, two possible alternatives have been identified by the Office of Information Security:

1. Purchase Windows 7 Extended Security Updates (ESU) licenses through EITS for the systems that will not be migrated. These licenses cost \$50 per system to cover patches in CY2020; licenses to cover

CY2021 will cost an additional \$100. The attached document describes how to purchase these licenses and how patching under these licenses will be accomplished. These licenses will allow agencies to keep Windows 7 desktops patched and operational through December 2021, six months into the next biennium, allowing sufficient time for replacement systems to be budgeted, purchased and deployed.

2. Request limited access, where the system will be locked down to access only essential systems and services. This option will not be available to all agencies, as the ability to lock down system access to this degree is largely affected by the number of systems involved and the network architecture within the requesting agency. Therefore, these requests will be reviewed for technical feasibility on a case-by-case basis.

Either of these alternative plans will require an exception request, approved by the agency Information Security Officer and the Chief Information Security Officer. Requests for exception should reference State Standard S.5.07.01. Agencies should submit a single request to cover all systems needing exception rather than individual requests for each system; the request must be accompanied by a spreadsheet listing, at a minimum, the system name and property tag number of systems covered by the request.

It is worth noting that State Security Standard S.2.05.02 – Suspension of Services – provides for the suspension of access to Silvernet in case of violation of “Nevada Revised Statutes (NRS), Federal or international law, State or agency security policies, standards and procedures (PSPs).” (Section 6.1.E) A filed and approved exception request is the proper way to deal with situations where an agency is unable to comply with state security policy or standards.

Should you have any questions, please feel free to contact me at rwdehnhardt@admin.nv.gov or 775-684-7322.

CC:

Michael Dietrich, State Chief Information Officer
Agency IT Managers

Attachments:

EITS ESU License Instructions

State Security Standard S.5.07.01, IT Operating System Patch Upgrade Management
