



Wisconsin Elections Commission

201 West Washington Avenue | Second Floor | P.O. Box 7984 | Madison, WI 53707-7984
(608) 266-8005 | elections@wi.gov | elections.wi.gov

2022 Election Security Subgrant Compliance Standards

Appendix B

I. Background

- A. Securing state information systems is critical. Wisconsin residents rely on the state, counties, and municipalities to deliver services reliably and safely. Cyber-attacks are a continuous threat to the delivery of those services. The state needs your help to protect state systems and residents' information.
- B. Cyber threats commonly focus on the weakest link within systems, primarily the people using those systems. This document provides basic guidelines to reduce risks and ensure fundamental cybersecurity standards.
- C. Terms Defined.

Compliant Device: a device that meets minimum security standards outlined in section II.A. below.

Managed Device: a device that is receiving managed IT service. Someone else (usually a private computer company) is managing the device security.

Managed IT Service: ongoing IT support meeting the requirements outlined in section II.B. below.

Managed Service Provider: a company offering managed service to customers; usually for a monthly fee.

II. Baseline Security Standards for Access to and Use of State Elections Systems

A. Compliant Computer Hardware and Software that Meets the WisVote Policy Requirements.

Jurisdictions must use grant funds to meet this requirement before spending funds on any other need. The 2022 Election Security subgrant will allocate \$600 for the purchase of one device by the jurisdiction. Compliant hardware and software must meet the following standards:

- i) Computers using a currently supported operating system (OS).
 - a. Windows 11, Windows 10 (or Windows 8.1 is non-compliant effective 1/10/23)
 - b. MacOS 10.15 Catalina (or newer)
 - c. Consult with an IT professional or call the Elections Help Desk if you run another operating system (Linux, Chrome OS, etc.).
 - d. See Appendix C for information on how to check your Operating System.

Wisconsin Elections Commissioners

Don M. Millis, chair | Marge Bostelmann | Julie M. Glancey | Ann S. Jacobs | Robert Spindell | Mark L. Thomsen

Administrator
Meagan Wolfe

- ii) Computers with current:
 - a. Patches / Firmware (no later than 30 days of release by vendor). Ensuring your operating system is up-to-date will generally take care of this requirement. For smaller jurisdictions automatic updates will fulfill this requirement so long as they are not delayed or disabled.
 - b. Antivirus software.
 - c. Anti-spam and anti-spyware software.
 - d. Web filtering software to protect against malicious websites.
 - e. Merely possessing anti-malware software is not enough. You must download updates regularly to ensure your system is protected from the latest threats.
- iii) Computers owned or controlled by the jurisdiction. While the WEC respects and permits remote work and work-from-home arrangements, jurisdictions must have **at least one device** that is under the jurisdiction's legal control to meet this baseline standard. This allows a jurisdiction to remain compliant in the event of staff turnover.

The WEC installs endpoint verification testing in WisVote to verify compliance upon login.

How to Achieve Compliance:

- i) Purchase a Compliant Hardware Device. If a jurisdiction does not have compliant hardware or software/operating system it must use the 2022 Election Security Subgrant funds to achieve compliance. Local jurisdictions may use their funds to purchase a compliant hardware device from vendors on the state contract or from any other vendor or local retail store they choose. More information regarding the purchase of compliant devices is included in Appendix C.
- ii) Update Your Operating System to Windows 11 or Windows 10. One option is to update the operating system on the computer currently used to access WisVote. For example, if the jurisdiction is currently using the Windows 8.1 operating system, and the computer and software are otherwise compliant, \$200 of subgrant funds may be requested to upgrade the operating system. Additional information regarding updates to operating systems is included in Appendix C. Note that this option requires ongoing IT support to ensure systems stay current.

B. IT Support Capable of Maintaining Minimum Standards

Jurisdictions must certify that they are able to maintain their hardware and software in accordance with the policies above through 2024. This means that each jurisdiction must either possess professional, full-time IT staff, or obtain managed support through a managed support provider. The IT support must agree to maintain current patches, firmware, anti-virus software, and web filtering software. IT support must also notify the WEC of any cybersecurity incidents involving the jurisdiction's clerk or election systems and agree to receive Cyber Alerts from the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). More information on these requirements is provided in Appendix C. The 2022 ES subgrant will allocate \$600 towards managed support costs that meet baseline standards. Jurisdictions must certify compliance by completing the WEC Security Subgrant Compliance Form (Appendix A), however the WEC will monitor the patch level of devices used to access WisVote. If a device is not in compliance with

patching requirements, the WEC will follow up with the municipality to help achieve compliance. While the jurisdiction is awaiting a patch, the user may be denied access to WisVote until the patch is complete.

How to Achieve Compliance:

- i) Obtain a Managed Service Provider. A jurisdiction may also use their 2022 ES subgrant funds to contract with a managed IT support provider to maintain minimum standards. The local election jurisdiction will then need to certify that it has compliant IT support and provide the documentation detailing their support with their Election Security Subgrant Compliance Form (Appendix A). More information about choosing a support provider is included in Appendix C.
- ii) Possess in-house, shared, or contracted IT staff that provides all the services listed in Appendix C. The local election jurisdiction will then need to certify that it has compliant IT support and provide the documentation detailing their support with their Election Security Subgrant Compliance Form (Appendix A).

C. Completion of a Contingency Plan

The WEC recommends every municipality maintain a contingency plan in the event of an election security crisis, and the completion of a plan is a requirement for the subgrant program. To assist with this process, information about preparing a sample contingency plan can be found in Appendix C.