

Security Recommendations for Electronic Voting Systems

adopted by the Wisconsin State Elections Board on June 23, 2006

Introduction and Scope

These recommendations apply to all memory devices, including, but not limited to, prom packs, memory cards or any other removable memory devices that can be programmed or function to store and transfer ballot images or tabulation data.

Nothing prohibits reuse of memory cards, though municipalities must comply with section 7.23(1)(g) Wis. Stats.: "Detachable recording units and compartments for use with electronic voting machines may be cleared or erased 14 days after any primary and 21 days after any election. Before clearing or erasing the units or compartments, a municipal clerk shall transfer the data contained in the units or compartments to a disk or other recording medium which may be erased or destroyed 22 months after the election to which the data relates."

The Wisconsin State Elections Board recognizes the need for flexibility when implementing these recommendations, and acknowledges that alternative means may be used to achieve and ensure the same level of security. Therefore, the State Elections Board will consider requests from municipalities and counties to implement alternative security procedures.

General Statements

1. Throughout the life of the voting system, the municipal clerk shall maintain control of all memory cards and keep a separate, perpetual, written chain-of-custody record for each memory card used with a voting system. Memory cards shall be stored securely at all times and each access and transfer shall be logged in the record.

Upon the agreement of the municipal clerk, the county clerk may store memory cards in secure location. In this instance, both clerks must maintain a separate, perpetual, written chain-of-custody records for each memory card used with a voting system.

An additional written log shall record everyone who accesses the voting system. This log shall include the name of the person, the date and time the access begins, the purpose of the access, and the time the access ends. Such documentation does not apply to election day procedures.

The recommended, but not required, practice is that memory cards shall at no time be in the possession of a single individual. Regardless of compliance with this recommended practice, a separate, perpetual, written chain-of-custody record must be maintained for each memory card used with a voting system.

2. Each memory card shall have or be assigned a unique and permanent serial number. If the memory card does not have a permanent and fixed serial number affixed by the



manufacturer, a clerk may affix a label to the cards which contains the clerk's original signature.

3. The municipality shall use controlled, serialized seals that are tamper-resistant and resistant to inadvertent breakage along with a written log of all seals and associated serial numbers. The municipal clerk, or county clerk if applicable, should maintain a written log that records which memory cards and which serialized tamper-evident seals are assigned to which voting stations or units.
4. If applicable, the municipal and/or county clerk(s) shall maintain an additional written inventory of all keys that may be used to gain access to the voting systems. The municipal and/or county clerk(s) shall keep a perpetual, written chain-of-custody record for all such keys.
5. These procedures shall be followed for each election, recount, or for any other situation in which the voting system or memory cards must be accessed.

Pre-Election Procedures

6. The municipal clerk, or county clerk if applicable, shall check the locks and security seals and compare to the logs to verify who accessed the voting systems or memory cards since the previous election.
7. Memory cards shall, if possible, be programmed to print a list of the software and firmware versions of the voting system on each beginning-of-election-day zero report and end-of-day zero report. This information shall also be printed on any reports generated during the pre-election testing, including the public test.

For existing systems that cannot accommodate this requirement, this information may be recorded from the system start-up screen, either by municipal or county staff during the pre-election testing or by election inspectors during election day.

The records for both the pre-election test and election day reports must be maintained by the municipal or county clerk.

8. Except when necessary to program, test, or operate the system, each system must be closed and locked with a tamper-resistant seal which can be tracked using a unique and permanent serial number. Each input slot or access port, including serial or modem ports, must be closed and locked using a tamper resistant seal which can be recorded using a unique and permanent serial number.

Alternately, these slots or ports may be disabled, with written documentation of the dates and times maintained by the municipal or county clerk.

Any door by which access can be gained to the system controls must be closed and locked using a tamper-resistant seal which can be tracked using a unique and permanent

serial number. The municipal or county clerk shall maintain a written record of such serial numbers.

9. Once a memory card is programmed for the election, it shall be immediately inserted into its assigned unit and sealed against unauthorized access with a serialized, tamper-evident seal which can be tracked using a unique and permanent serial number. The voting station shall not be set into election mode until after the memory card is sealed inside.

Alternately, memory cards may be locked in a secure location with controlled access; written documentation of access to programmed memory cards must be maintained.

10. The municipality or county should obtain a signed "Certificate of Performance Compliance: Memory Card Security" from each vendor that provides voting systems, equipment, programming services, or memory cards to the municipality.

Election Day Procedures

11. On Election Day, before any ballots are cast on any unit, the integrity of the tamper-evident seals shall be verified by the chief election inspector before accessing compartments containing the memory card and unit power switch. The chief election inspector shall record this information on the Inspectors' Statement (EB-104) and chain-of-custody document for the memory card.
12. Once the polls have been opened on Election Day, ballot removal from an optical scan machine or paper roll removal or replacement on a Direct Recording Electronic (DRE) must be conducted with at least two election inspectors (or other sworn election team members appointed by the municipal clerk) present. The removal process, names of the election inspectors or sworn election team members, and time must be recorded on the Inspectors' Statement (EB-104).
13. In post-election mode, election officials must print the results report before the removal of the memory card from the voting stations or units. If additional reports other than the results reports are available, these reports must also be printed before the removal of the memory card.
14. One copy of the results report and the memory cards shall be secured in a separate, sealed container or envelope by the chief election inspector. The chief election inspector and two additional election inspectors shall sign their names across the seal of the secured envelope or container. The memory cards shall be promptly returned to the municipal clerk.

If results are transmitted by modem, the municipal clerk may access the memory card for transmission purpose, but must reseal and sign his or her name across the seal of the secured envelope or container. Before transmitting the results via modem, the clerk must print an additional results report from the system and record the transmission time on the Inspectors' Statement (EB-104).

As an alternate procedure, the memory cards may remain sealed in the voting stations or units. The numbers of the security seals shall be recorded on the Inspectors' Statement (EB-104).

Post-Election Procedures

15. After each election, the clerk responsible for storing the voting system shall conduct an inspection to ensure that each system is locked and secured. Written documentation shall note the date and time of the inspection and any applicable security seal numbers.
16. Prior to the next election or recount, the municipal clerk, or county clerk if applicable, shall inspect the security seals to ensure that each seal number matches the initial ending documentation from the previous election.

**CERTIFICATE OF PERFORMANCE COMPLIANCE:
MEMORY CARD SECURITY**

The undersigned supplier of voting system services certifies that documented procedures for assuring memory card security and chain of custody have been provided to the Wisconsin State Elections Board and have been utilized while the supplier had control or access the memory cards with the following serial numbers:

The undersigned further certifies that no codes, files, programs or language have been added to the memory card that deviate in any way from the approved version in escrow with the Wisconsin State Elections Board. The undersigned understands and agrees that any deviation from this agreement subjects the undersigned to: (1) de-certification of any or all voting systems or services provided by the undersigned supplier; (2) a rebate of full purchase price to all municipalities which have purchased said system; and (3) any applicable civil or criminal penalties that may be available to the purchaser of such services or the State Elections Board, including, but not limited to the election fraud provisions provided in section 12.13 Wis Stats.

**Procedures for requesting approval from the State Elections Board for the use of
alternative security procedures**

1. Procedures shall be submitted in writing to the State Elections Board (SEB) and received by that office for approval no later than sixty (60) days before the election date. The SEB shall review the alternative procedures and shall either approve the procedures submitted or notify the designated election official of recommended changes.
2. Approved security procedures will remain in effect until the municipality requests, in writing, a revision or the SEB determines a change necessary.
3. Revision requests to previously filed security procedures shall clearly state which part of the procedures previously filed have been revised.
4. Alternative security procedures shall, at a minimum, detail:
 - a. Physical security of election equipment, software and firmware, and memory cards including but not limited to:
 - i. Locking mechanisms and seals;
 - ii. Chain-of-custody procedures and logs
 - iii. Equipment maintenance procedures
 - b. Verification security including but not limited to:
 - i. Pre-election verification of software and firmware versions
 - ii. Pre-election zero status

Receipt of a signed "Certificate of Performance Compliance: Memory Card Security" from each vendor that provides services to the municipality.