Jon Husted
Ohio Secretary of State
180 East Broad Street, 16th Floor
Columbus, Ohio 43215
Tel: (877) 767-6446 Fax: (614) 644-0649
www.OhioSecretaryofState.gov

DIRECTIVE 2012-46
September 14, 2012

To: All County Boards of Elections
Directors, Deputy Directors, and Board Members

Re: Security of Board of Elections Office, Security, Proper Storage, and Transport of Voting Equipment, Ballots, and Election Data Media

SUMMARY

This Directive outlines the measures that each board of elections must implement to ensure the security of its office and the security, proper storage, and transport of its voting equipment, ballots, and election data media. Specifically, it addresses the following topics:

- Security of the board office;
- Secure and proper storage of voting equipment;
- Inventory of voting equipment;
- Secure and proper storage of ballots and election data media;
- Inventory of ballots;
- Secure transport and delivery of voting equipment and election day supplies;
- Polling place security and emergency response;
- Secure return of ballots and election day supplies; and
- Security of voting system and tabulation programs and software.

This Directive rescinds and replaces Directives 2008-25, 2008-56, 2008-54[1], 2008-57, 2008-68, 2008-72, and 2008-73, 2011-19, and Advisory 2008-20.

INSTRUCTIONS

A. Security of the Board Office

Each board of elections is required to adopt a policy regarding the overall security of its office. This policy already may be contained, in whole or in part, within the board's Election Administration Plan (EAP). Boards of election must review their plan to ensure that it is complete and consistent with this Directive.

[1] Please see Directive 2011-19 for guidance on encoding key cards.

When adopting its security policy, a Board must consider, at minimum, the following:

1. How it can best prevent unauthorized access to the board office;
2. How board staff will register and supervise visitors;
3. How the Board can restrict access to those areas of its office that house voting equipment, election materials, and its tabulation and voter registration servers;
4. How will the board regularly audit its records and procedures to ensure they are being followed; and
5. If there is a violation of the security policy, what is the reporting process?

B. Secure and Proper Storage of Voting Equipment

In addition to adopting a policy to address the overall security of the board office, each board of elections must adhere to the following guidelines in storing voting equipment at its office or other designated site whenever the equipment is not in use.

- To prevent damage and maintain the integrity of the equipment, each board of elections must store its voting equipment properly in a secure, clean, and climate-controlled area.

- Physical security of voting equipment in the storage area must be maintained at all times. Access to the equipment should be limited to the least number of board personnel as possible.

- All equipment, along with the cases, cabinets, and/or shelving units that house the equipment, must be locked under a dual-control lock system, such that any access to the equipment requires a bipartisan team. The Director or Designee of the same political affiliation must hold one key or lock combination and the deputy director or designee of the same political affiliation must hold the other key or lock combination.

- The identification of any visitor, vendor, or maintenance personnel must be verified before he or she may be granted access to the equipment storage area. The Board must keep a log of the name of each visitor, vendor, or maintenance person who enters the area, along with the date and time of his/her entry and exit. Visitors should be monitored at all times. The best method for access control is one that uniquely identifies the person, authorizes entry, and logs the date and time of access (i.e., badges, door entry access devices, and video monitoring system).

- The storage area must be equipped with a monitored, alarmed smoke detection system and the proper fire extinguisher(s) or suppression system, so, if a fire occurs, it may be detected, extinguished, or suppressed as quickly as possible. Board personnel must be trained on how to respond to a fire in the storage area.

- All voting equipment must be stored properly. Each Board must contact the manufacturer of its voting equipment and request and review the voting equipment or system manual for instruction on the proper storage of the equipment. Please note that improper storage of the equipment may affect the voting system maintenance agreement and/or the equipment’s warranty.

- The storage area must be clean and free of excess dust, debris, and pests. The Board should routinely inspect and clean the area. Voting equipment must not be stored on the ground in an area prone to flooding or in any area where liquid accumulates.

C. Inventory of Voting Equipment

The Board must inventory all of its voting equipment and maintain a list of each item of equipment and its corresponding serial number. Additionally, for each piece of equipment, the Board must retain the following:

- Invoice, purchase order, or other documentation of the purchase of the equipment;
- Chain of Custody Log for at least 90 days following every election;
- Record of the equipment's usage (i.e., the date and location of use and the individual(s) using the equipment);
- A report of any damage to or unauthorized handling of the equipment; and
- Any repair history (when, where, by whom, for what purpose, and the outcome) and documentation of the repair.

The inventory list must be maintained and reviewed on a regular basis by the board's Director and Deputy Director.

D. Secure and Proper Storage of Ballots and Election Data Media

For purposes of this section, ballots and election data media includes, but is not limited to the following:

- Optical scan ballots prepared by a vendor or printed in house by the Board for use in an upcoming or previous election;
- Blank ballot stock for a Ballot on Demand (BOD) printer;
- All memory cards or PCMCIAs;
- CDs or USB drives that house election results;
- VVPATs;
- Personal Electronic Ballot (PEB) cartridges; and
- eCM tokens.

When not in use, all ballots and election data media also must be stored properly in a clean and climate-controlled environment that is equipped with a monitored, alarmed smoke detection system, and the proper fire extinguisher(s) or suppression system following the guidance provided above for the storage voting equipment. These items must not be stored on the ground in an area prone to flooding or in any area where liquid accumulates. Food and beverages should never be stored or consumed within the storage area.

Access to ballots and election data media must be restricted to authorized personnel only. These items should be segregated and stored in a separate, locked room or storage unit (e.g., cabinet) designated for that purpose. As with voting equipment, ballots and election data media must be

locked under a dual-control lock system. An explanation of a dual-control lock system is provided above under "Secure and Proper Storage of Voting Equipment."

Ballots must be stored as recommended by the printer (or, if storing blank ballot stock, as recommended by the manufacturer of the blank ballot stock). They must be stored in protective cases, containers, or if recommended by the printer or manufacturer, in their original packaging.

Election data media should be stored in a sleeve or case and should be marked so that each item is easily identifiable.

E. Inventory of Ballots

The Board must inventory all ballots by implementing the following procedures:

- If optical scan ballots are printed by an outside source, the Board must maintain a list of the ballot styles and the number of ballots for each style that are delivered to the Board by the printer. The Board must document any discrepancy between what was ordered and what was received and the steps taken to rectify the discrepancy. The Board must also maintain a list of the sequence numbers of the ballots received, the number and sequence number range of the ballots that will be provided to each precinct, and number and sequence number range of the ballots for absentee and provisional voting. The Board must document the disposition of each ballot (i.e., voted, unvoted, or spoiled).

- If optical scan ballots are printed in house via a BOD printer, the Board must document the use of each sheet of blank ballot stock.[2]

A Chain of Custody Log must be used to document the delivery of optical scan ballots to each precinct.

F. Secure Transport and Delivery of Voting Equipment and Election Day Supplies

Each board of elections must arrange for the delivery of voting equipment to polling locations prior to or on Election Day. If voting equipment will be delivered to a polling location prior to Election Day, the Board must arrange for the security of the equipment at the polling location. The storage of voting equipment at a precinct election official's home, vehicle, or place of employment is prohibited, and a precinct election official must never retain custody of voting equipment overnight.

At a polling location, voting equipment must be stored in the manner recommended by the voting equipment manufacturer and in a clean and climate-controlled environment. The equipment must not be stored on the ground in an area prone to flooding or where liquids accumulate.

[2] No board of elections shall use a ballot-on-demand system unless each ballot printed by the system includes a tracking number. R.C. 3506.20(B).

If memory cards are inserted into the voting machines when they are delivered to a polling location or transferred to a precinct election official, the Board is required to use tamper evident seals to allow detection if the memory card is tampered with while in the machine. The seal must be unique to each machine with a documented, unique identifier that corresponds to the particular voting machine. Documentation of the unique identifier for the tamper evident seal as it corresponds to a particular voting machine should be maintained on three lists. Two lists must be retained in a secure location at the board office, with one kept by the Director and the other by the Deputy Director.

Upon set up and closing, precinct election officials must inspect all pieces of voting equipment that are assigned to their precinct for any physical damage. Precinct election officials must document the inspections on a maintenance/event log provided by the board of elections and must specifically note any signs of damage or tampering discovered on the equipment or cases used to house the equipment.

Additionally, boards of elections must use a chain of custody log (SOS Form 400 or local equivalent) to document the exchange of custody of voting equipment, election supplies, and/or ballots. Boards of Election should train precinct election officials on inspection of tamper evident seals so they know what to look for when inspecting the equipment.

G. Polling Place Security and Emergency Response

Precinct election officials must maintain control over all voting equipment, keys, memory cards, ballots, and all other election supplies at all times. Any suspicious activity or damage to the equipment must be reported to the board immediately. The Board must provide each presiding judge with a list of persons to contact in the event of an emergency.

Precinct election officials must be instructed that, in the event of an emergency, their first priority is the safety of the electors and other election officials. Precinct election officials should remove voting equipment, election supplies, and ballots only if it may be done safely. If any voting equipment, election supplies, and ballots are removed from a polling location, at least one (preferably two, one of each major political party) must remain with the equipment and supplies at all times.

H. Secure Return of Ballots and Election Day Supplies

At the close of polls, all ballots and election supplies (i.e., pollbooks, poll lists, tally sheets, election reports, and other materials) must be returned by a bipartisan team to the board of elections office or other location designated and staffed by the Board. The bipartisan team must consist of the presiding judge and an employee or appointee of the board who is a member of a different political party than the presiding judge and "has taken an oath to uphold the laws and constitution of this state, including an oath that the person will promptly and securely perform the duties [of promptly and securely transporting and delivering ballots and election supplies to the board of elections]."[3]

[3] R.C.3505.31.

When transporting ballots and election supplies, the bipartisan team must travel in the same vehicle. The Board is permitted to have one or more additional persons, such as a law enforcement official, accompany the bipartisan team. One bipartisan team may transport the ballots and election supplies for an entire multi-precinct polling location.

I. Security of Voting System and Tabulation Programs/Software

No voting machine[4] or component of a voting system may be connected to the internet. A voting system includes the total combination of mechanical, electromechanical, and electric equipment, including software or firmware required to program, control, and support the equipment that is used to: set up elections, define ballots cast, receive voting data from polling places, count votes, report or display election results, and maintain and produce any audit trail information. The board's voter registration server is not considered a voting machine or component of a voting system for purposes of this section.

Voting machines or components of a voting system may only be connected via a local computer network cable to the central tabulating system (a closed local network) for the purpose of creating or uploading memory cards, ballots definitions, precinct results, and other required tasks. Additionally, voting machines in a polling location may be connected to a closed local network.

Election results, ballot definitions, or other similar information must never be transferred to a voting system via the internet (except that blank ballots may be transmitted to a UOCAVA voter via the internet or facsimile).

No one may download or install software or firmware on a voting machine or components of a voting system without prior approval from the Secretary of State's Office.

J. Passwords

In order to maintain the proper security of the voting equipment and central tabulating system the following password protocols must be used:

- A BIOS password shall be required for all vote tabulation sever systems, forcing users to enter a correct BIOS password in order to boot the machine.
- All central tabulating systems must be password protected. At a minimum the passwords must be composed as follows:
    - The password must be split with authorized Republican personnel possessing half of the password and authorized Democratic personnel possessing the other half of the password;
    - The entire password must be at least 12 characters or the minimum number that the system will accommodate, whichever is greater;
    - Each half of the password must have a number included in it;
    - Each half of the password must include one non-alphanumeric character;
    - Each half of the password must include mixed-case letters; and

[4] R.C.3506.22.

  - The entire password must have no more than two consecutively repeating characters.

- Both the BIOS and central tabulating system software passwords must be required to be changed prior to every election.
- Both the BIOS and central tabulating system software passwords must require 10 unique passwords prior to reuse of a prior password.
- Both the BIOS and central tabulating system passwords shall be distributed to only authorized users. This means that the posting of the either half of a password on a monitor or keyboard is strictly prohibited.
- The system shall log out users after five minutes of inactivity.

K. User Account Management

For all IT systems containing voter information and central tabulating systems, boards of election must require every user to have a single unique user ID and a personal password unique to that user. This ID and password must be required for multi-user access to computers and networks.

L. Access Log

Directors and Deputy Directors shall regularly monitor the access logs maintained by their election management systems and voting system servers. When checking these logs, Directors and Deputy Directors should look for any unusual or suspicious access or activity on the system. Examples of this kind of activity would be accessing the systems at unusual hours and with unusual frequency. Electronic logs must not be disabled.

M. Third Party Access to Voting System

Board policies on voting system server security must prohibit individuals who are not employees, contractors, or consultants of the board of elections or Secretary of State's Office from being granted a user ID or otherwise be given privileges to access any network or component of the election system within the board offices or at a satellite location, unless the written approval of both the Board's Chairman and Director have been obtained.

Before providing to any third party access to any network or component of the election system within the board's offices or at a satellite location, written documentation defining the following shall be executed: The scope of work and authorization for access to any network or component of the election system within the board offices or at a satellite location; relevant terms, including the name of a responsible manager at the third party organization; and the timeframe, with starting and ending dates and times, if applicable, for access.

If you have questions regarding this Directive, please contact Matthew Masterson at (614) 466-2585.

Sincerely,

Jon Husted