

DIRECTIVE 2008-73

August 26, 2008

**TO: ALL COUNTY BOARDS OF ELECTIONS
MEMBERS, DIRECTORS AND DEPUTY DIRECTORS**

RE: Minimum Security Requirements of Vote Tabulation Servers

To further enhance the integrity of the election process in Ohio, the Secretary of State's office is directing all boards of elections to maintain minimum requirements concerning the security of vote tabulation servers.

Each board of elections shall develop and/or maintain a policy for account and password management for granting access to the server and access to related workstations, if any, for its election system. Each board of elections shall have a policy for maintaining sign-in documentation of server activity and related workstation activity, if any. The board shall also have a policy for monitoring election system activity through the use of audit logs and other security practices as may be established by the board or the Secretary of State.

All policies shall be based, at a minimum, on the requirements set forth in this directive. The policy must be reviewed at least annually and updated to conform to changes in board organization, structure, personnel, state law, Secretary of State directives and advisories, equipment, certification activity by the Board of Voting Machine Examiners, and other occurrences or changes that will affect the implementation of the board's policy.

The board of elections shall enforce all policies and procedures relating to the security of the vote tabulation server and related workstations.

PASSWORD MANAGEMENT

BIOS Passwords

A BIOS (Basic Input/Output System/Basic Integrated Operating System) password shall be required for all vote tabulation server systems, forcing users to enter a correct BIOS password in order to boot the machine. It is recommended that the password be split with authorized Republican personnel possessing half of the password and authorized Democratic personnel possessing the other half of the password. Each half of the password must be distinct (e.g. "vote1-vote2" is not acceptable) and shall not be known to anyone other than the authorized user.

Account Passwords

The password to the Election Management System must consist of a split password as described and recommended for the BIOS.

Password Complexity and Composition Guidelines

At a minimum, passwords must be composed as follows:

- The entire password must be at least twelve (12) characters, or the minimum number of characters that the specific vendor's systems will accommodate, whichever is greater.
- The entire password must include at least two numbers.
- The entire password must include at least one non-alphanumeric character.
- The entire password must have no more than two consecutively repeating characters or group of characters.
- The entire password may include mixed-case letters.

Each split password user will be required to provide one-half of the requirements as outlined above.

Password Aging

All users shall be automatically required to change their passwords at least prior to every primary and prior to every general election. This aging scheme is to encompass the above recommendations on maintaining a password history – users must not be able to re-use their old passwords as long as those passwords are in a password history list.

Password History

If the vote tabulation server system allows for the creation of a password history, the board of elections shall enforce a password history system. This is a method by which users are not permitted to re-use any of their last several passwords. The exact number of forbidden passwords in the history is usually configurable. When a system like this is available, users must not be unable to use their last ten passwords, at a minimum.

Responsible Management

Policies shall provide that passwords shall be distributed only to authorized users, and must not be contained in any other written documentation. This password creation policy must be applied to all user accounts on the server system software.

Time out/Log out

Policies shall address the issue of a time out/log out requirement for server access. If a user must step away from the server, it must be set to time out after a period of 5 minutes of idle non-use. Or, at any time a user must leave the server, he or she must be required to log out and re-log when returning to the server, or lock the server so that nobody else can access it.

ACCOUNT MANAGEMENT

Account Allocation

Board policies on voting system server security must require every user to have a single, unique user-ID (account name) and a personal, secret password. This user-ID and password must be required for access to multi-user computers and computer networks.

Users are never permitted to share accounts. Likewise, no group accounts are permitted to be created on an election system within a board office. Additionally, all account names must be

globally unique, so that no account name used in the past may be re-used again in the future (as opposed to eventual reuse in password history). The user-ID and password must be changed whenever office personnel changes.

Account for Third Parties

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.

IMPORTANT NOTE: The voting systems in use in Ohio have been certified with particular versions of software and hardware. No board shall cause or permit to be introduced into an election system any additional software, including updates or virus software, without the express written permission of the Secretary of State's office. Nor should any installation or update of software occur by connecting the election system to the Internet, in keeping with the requirements of R.C. 3506.23 and 3506.01(E), requiring that no voting machine, including a machine for the tabulation of votes, be connected to the Internet.

This ensures consistent configuration of election systems throughout the state as certified by the Ohio Board of Voting Machine Examiners and permits the Secretary of State to document and maintain records of system configurations throughout the state to ensure their consistency and reliability.

ACCOUNT MAINTENANCE

Logging

Board policies on voting system server security shall require that all activity of privileged (administrative) accounts on the election system, including the Election Management System, be documented on a sign-in form/list, that such activity shall be reviewed on a regular basis, and that the documentation shall not be altered.

Account Expiration

Board policies on voting system server security shall prohibit accounts from being left in a dormant state. Depending on whether the account owner will require the account in the future, the account may be either disabled or deleted completely.

ACCOUNT PRIVILEGES

Regular Account Privileges

Board policies on voting system server security shall require that user accounts be designated only for the minimum privileges corresponding to the responsibilities of the account's owner.

As a general rule, granting users unrestricted access subjects the system server to unwarranted risk. Users must not have the ability to modify data that is not directly within the scope of their employment responsibilities.

The creation of an initial user account, granting of additional privileges to users, and the revocation of account privileges must be required to be documented showing such activities were authorized and within the scope of the account owner's and authorizing party's employment or appointment.

Administrative Account Privileges

Board policies on voting system server security shall require that administrative privileges be granted only to authorized users. As part of this policy, each board of elections shall specify by position which account users (employees, contractors or consultants) are authorized to hold administrative privileges. Administrative accounts shall be separate from regular accounts on the election system, and administrative accounts must not be shared and must be used only for administrative duties that cannot be performed through the regular election system account. Since administrative accounts are privileged accounts, the number of privileged accounts must be kept to a minimum.

System Configuration

Board policies on voting system server security shall require that systems be configured and maintained so as to only allow authorized users to access them and to limit their access to the system to that which allows them to perform the actions consistent with their scope of work and the tasks necessary to perform such work.

SYSTEM MANAGEMENT PRACTICES

Inventory Documenting Election System Configuration in Each County

Each board of elections shall provide a report to the Secretary of State on a form prescribed by the Secretary of State inventorying the hardware used to operate its election system. This inventory shall include make, type and model, including numbers of each and date(s) of installation. In addition, the board shall provide in its inventory report the software and/or firmware maintained on its server, any workstations and voting equipment.

The inventory report shall include manufacturer name, name and function of software, including version and dates of installation and updates, if any, and shall correlate each listing of software to the hardware on which it is installed. If a particular software or firmware is installed on more than one hardware component, such as on voting machines, only one software or firmware listing for that type is needed and may be reported as installed on the related number of machines or components of the election system.

Initial Configuration

The Secretary of State will provide to the boards of elections the configuration of hardware and software, by voting system manufacturer type, as has been approved by the Ohio Board of Voting Machine Examiners for each type of election system in Ohio. Each board of elections shall compare this initial configuration to its existing configuration and detail on its inventory report how its configuration differs from the initial configuration, if at all.

Post-Configuration Installation/Maintenance

The Secretary of State is currently examining the use of antivirus software to be approved by the BVME for use on election system servers to determine the appropriate use of such software and its interaction, if any, with election system software and/or firmware. More information will be provided as it is available.

Board policies on voting system server security shall require that only the software necessary to operate each component of the system in a manner that is intended by the software's manufacturer be installed on servers, workstations and other election system components.

Board policies shall further provide that only persons authorized to access the administrative functions shall have access to modify system settings, and of such persons, no more than two persons, one of each of the two major political parties, shall be authorized to do so. In the event that a board relies on an outside contractor or consultant to undertake such system settings modification, two board employees, one of each major political party affiliation, shall observe the actions taken in modifying system settings for election system software or firmware.

Windows™ software components that are not used for operating the election system and that are installed on the server or on other hardware that is a part of the election system should be removed from the hardware components of the election system. This action is considered modification of the system settings for election system software and may only be performed by persons authorized as set forth above.

The system's Control Panel is of relevance to modifying the system's settings and is subject to the restrictions set forth in this section for modifying system settings.

MANAGEMENT TOOLS

Monitoring the state of the election system

Board policies on voting system server security shall require a sign-in form/list for the server and for any work stations to permit the board of elections to monitor which users have accessed the system, the date of access, for what duration, and for what function or purpose. The following matters should be part of any audit log, review and report on the use of the election system's servers and any server workstations to establish reliable and consistent monitoring of the system's activity:

- User Account Activity – consists of actions like logging in, logging out and running programs. Local Security Policies and the Windows Event Viewer can display this type of log data.
- State of System Services – consists of documenting which services are running on the server at what times, and assists in informing and maintaining server security.
- System Services Configuration – consists of documenting system services configuration, a review of appropriateness for the functions intended, and any related, necessary modification that can generally be executed through the system's Control Panel.
- File System State – consists of monitoring the contents and organization of a disk of the server. Awareness of the state of important files and programs related to the functioning of the system enhances security and performance of the system. Various classes of tools exist to help administrators understand and track activity on the server's file system.

Boards of elections are encouraged to work with the Secretary of State regional IT liaisons as well as the regional liaison assigned to their county to comply with these measures.

Log System Activity

Documentation of the log system activity as outlined above is required to ensure monitoring of all election system activity and to ensure its proper operation and integrity. **Audit logs for a system server or for system workstations are not permitted to be turned off, suspended, or disabled, and board policy must specify this.**

LOGGING PRACTICES - CLASSES OF LOG DATA

Administrator Activity

Administrator activity is administrator-account login and logout events and actions taken by the administrator during the login session. This information can be found in the Windows Event log. Various settings can be adjusted with Windows' local policy editor.

User Activity

User activity is user-account login and logout events and actions taken by the user during the login session.

Application Activity

Application activity is errors or events invoked by system applications and third party applications running on the system. It also includes logs generated by the applications.

ACCESS TO USER LOG DATA

Log data shall only be viewable according to policy established by the board of elections or as necessary by Secretary of State staff.

USER LOG REVIEW PROCESS

Administrators must review logs on a fixed schedule, as established by board policy, at least both before and after an election.

USER LOG RETENTION REQUIREMENTS

Logs are kept in a database on the server. **User logs must be enabled at all times and are not permitted to be turned off, suspended or disabled.** A backup of the database must be created after the official count after an election and stored on a CD-ROM. It is best to maintain this information on separate CD-ROMS per election or per type of election. This CD-ROM must contain the log of the activity for that database during the election process. The database back up must be retained by the board of elections for a period of not less than two years in a secure location with access that requires two employees, each of one of the two major political parties..

MALWARE PREVENTION

“Malware” refers to viruses and “Trojan horses.” Adhering to the following practices can eliminate threats presented by malware:

- Controlling what media, e.g. CD-ROMs, thumb drives, USB devices, etc., enters and leaves the location of the server, any related workstations and voting equipment.
- Situating the server in a secure location with documented and limited access to the server and any related workstations.
- Adhering to recommendations about operating only necessary applications on the servers, which may be common vectors of infection or interference.
- Maintenance of the servers and appropriate operating system-specific “bug” fixes and patches in conformity with Secretary of State guidance and Ohio Board of Voting Machine Examiner testing and certification.
- No installation or update of software may occur by connecting the election system to the Internet, in keeping with the requirements of R.C. 3506.23 and 3506.01(E), requiring that no voting machine (including a machine for the tabulation of votes) be connected to the Internet.
- All media, e.g. CD-ROMs, thumb drives, USB devices, etc. should be formatted or have all data deleted from them before being inserted into the server or component of the election system, unless otherwise authorized by action of the board or by the Secretary of State.

CONTINGENCY PLANNING

Planning Fundamentals

Because of the sensitive nature of the information being processed – the votes of our citizens – boards of elections must cultivate an attitude of particular care in the administration of the election system and its components, including voting machines and its software and firmware.

Plan Maintenance

Boards of elections are required to prepare, periodically update and regularly test emergency response plans for preserving the operation and records of its election system, including the ballots and records relating to persons who have voted in prior elections for which federal and state records retention schedules require maintenance of this information. These plans must provide for the continued operation of critical systems in the event of an interruption, including natural disasters, attacks or acts of war, or degradation of service.

Plan Execution

When a board of elections has credible reason to believe that the election system has been compromised, the server and any related or potentially affected components of the election system must be isolated from other components on any election system network. Boards of elections shall allow access to Secretary of State personnel and their designees to assist in securing equipment, software, records, and other materials and information relevant to preserving the records of voting and to assist in resolving issues related to the integrity of the election system and the election process.

Plan Dissemination

Boards of elections must maintain the documentation required by this policy, including contingency planning documentation, and provide for training in these procedures and documentation for staff of the board. Contingency plans must be reviewed at least annually and updated to conform to changes in board organization, structure, personnel, state law, Secretary of State directives and advisories, equipment, certification activity by the Board of Voting

Machine Examiners, and other occurrences or changes that will affect the implementation of the board's policy.

If you have any questions concerning this directive, please contact an elections administrator at 614-466-2585 or via e-mail.

Sincerely,

Jennifer Brunner