

SECRETARY OF STATE[721]

Notice of Intended Action

Twenty-five interested persons, a governmental subdivision, an agency or association of 25 or more persons may demand an oral presentation hereon as provided in Iowa Code section 17A.4(1)“b.”

Notice is also given to the public that the Administrative Rules Review Committee may, on its own motion or on written request by any individual or group, review this proposed action under section 17A.8(6) at a regular or special meeting where the public or interested persons may be heard.

Pursuant to the authority of Iowa Code sections 47.1 and 17A.4, the Secretary of State hereby gives Notice of Intended Action to amend Chapter 22, “Voting Systems,” Iowa Administrative Code.

These amendments are necessary to ensure computers used to tabulate election results are secure and that county commissioners acknowledge risks associated with connecting election computers to the county network or to the Internet.

Any interested person may make written suggestions or comments on the proposed amendments on or before February 10, 2015, by contacting Carol Olson, Deputy Secretary of State, Office of the Secretary of State, First Floor, Lucas State Office Building, Des Moines, Iowa 50319. Persons who want to convey their views orally should contact the Secretary of State’s office by telephone at (515)281-0145 or in person at the Secretary of State’s office on the first floor of the Lucas State Office Building.

Requests for a public hearing must be received by February 10, 2015.

After analysis and review of this rule making, no impact on jobs has been found.

These amendments are intended to implement Iowa Code section 52.5.

The following amendments are proposed.

ITEM 1. Amend subrule 22.50(1) as follows:

22.50(1) Staff access. The security policy shall describe who shall have access to the voting equipment, including the computers used in the commissioner’s office to prepare ballots and voting equipment programs or to compile election results.

ITEM 2. Amend subrule 22.50(2) as follows:

22.50(2) Computers. For security purposes, computers used in the commissioner’s office to prepare ballots and voting equipment programs or to compile ~~and report~~ election results ~~should~~ shall not be used for any other function and ~~should~~ shall not be linked to any computer network or to the Internet unless the commissioner has on file in the office of the state commissioner a current Election Computer Risk Acceptance Form indicating acceptance of this security risk. The Election Computer Risk Acceptance Form, once submitted, is current until the end of the next even-numbered calendar year.

a. If the election computers are linked to a network or to the Internet, the commissioner shall use a firewall to filter network traffic. Data transmissions over the Internet shall be encrypted and password-protected. Information posted to a Web site shall not be considered transmission of data over the Internet.

b. Access to the computer(s) used to prepare ballots and voting equipment programs or to compile election results shall be limited to persons specified by the commissioner in the written security policy. The level of access granted to each person identified in the policy shall be included in a written security policy specified.

(1) ~~Uniqueness. Every ID and password~~ The usernames and passwords for each user authorized in the security policy shall be unique. The creation of generic or shared user-IDs usernames is specifically prohibited. Each user shall have exactly one user-ID username and password, except where job requirements necessitate the creation of multiple IDs usernames to access different business functions.

(2) No change.

(3) ~~Generic user-IDs usernames.~~ Staff members with generic user-IDs usernames are not allowed to sign on to voting systems.

(4) No change.

c. No change.