

721—22.50 (52) Voting system security. Each county shall have a written security policy. The policy shall include detailed plans to protect the election equipment and data from unauthorized access. The policy shall describe the methods to be used to preserve the integrity of the election and to document the election process.

22.50(1) Staff access. The security policy shall describe who shall have access to the voting equipment.

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 not be used for any other function and should not be linked to any computer network or to the Internet.

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 shall be limited to persons specified by the commissioner in the written security policy. The level of access shall be included in a written security policy.

(1) Uniqueness. Every ID and password shall be unique. The creation of generic or shared user IDs is specifically prohibited. Each user shall have exactly one user ID and password, except where job requirements necessitate the creation of multiple IDs to access different business functions.

(2) Authority. Each user shall be granted only the level of access specifically required by the user’s job. Use of “Administrator,” “Super User,” “Security Administrator,” or “SA” levels of authority shall be severely restricted.

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

(4) Password standards.

Account Policy	Recommended Setting
Maximum Password Age	90 days
Minimum Password Age	2 days
Minimum Password Length	8 characters
Enforced Password History	6 passwords (last 6 cannot be used)
Account Lockout (number of unsuccessful log-on attempts)	3 bad attempts
Account Lockout Duration	6 hours
Reset Account Lockout Counter After	6 hours

c. Hardened operating system. For security purposes, users of Election Systems & Software, Unity 3.4.0.1 and Democracy Suite 4.6 shall harden the operating system on the computer on which the election management system is housed according to the specifications of the vendor and the recommendations of the county information technology department (if any).

22.50(3) Evacuation. If it is necessary to evacuate the election office, a satellite absentee voting station or a polling place, the precinct election staff or the election officials shall immediately attempt to notify the commissioner and take the following actions:

a. Keep people safe.

b. If possible, gather and secure voted ballots, election equipment and critical election documents.