SCORE
End User Acceptable Use Policy

PURPOSE:

The SCORE system maintains sensitive information that requires protection. This policy establishes a standard to protect sensitive personally identifiable information (PII) contained in the Colorado Department of State's SCORE system. . Under Colorado law, PII includes:

- Electronic mail addresses (Section 24-72-204(2)(a)(VII), C.R.S.)
- Addresses and telephone numbers of students in any public elementary or secondary school (Section 24-72-204(3.5)(a)(VI), C.R.S.)
- The address of any election in confidential status (Section 24-72-204(3.5)(c), C.R.S.)
- The request for confidentiality filed by an elector in confidential status. (Section 24-72-204(3.5)(f), C.R.S.)
- Original signatures, social security number, month of birth, day of month of birth or identification numbers (Section 24-72-204(8)(a), C.R.S.)
- All information regarding electors who have completed the registration procedures applicable to Address Confidentiality Program participants. (Section 24-30-2108(3)(a), C.R.S.
- All information relating to pre-registrants who did not attain the age of 18 years by the date of the special district election. (Section 1-2-227(2), C.R.S.)

SCOPE:

This policy applies to any person who accesses or uses the SCORE system and any associated equipment that is used to manage, access, and or monitor the SCORE system. All Colorado SCORE users must sign and agree with this policy. [Reference Colorado Information Security Act (C.R.S. 24-37.5, Part 4) and State of Colorado Cyber Security Policies - http://www.oit.state.co.us/ois/policies]

INDIVIDUAL RESPONSIBILITIES:

An individual accessing the SCORE system must comply with the following standards and provisions:

- Users are strictly prohibited from sharing passwords or multi-factor-authentication devices including grid cards or tokens.
- Users must use complex passwords and they must comply with the following requirements:
  - Be at least nine characters in length.
  - Contain three out of the four following items:
    - Lower-case letter
    - Upper-case letter
    - Number
    - Symbol
  - Not contain the user's name or username.
  - Avoid using simple dictionary words without proper length and complexity. Passwords should be generated from pass phrases or uncommon word associations.
    - Example: **T**he **l**azy **D**og **w**as **u**nder **t**he **p**orch **t**his **m**orning**!** equates to **"TlDwutptm!"**
    - Example: Horse79!Staple! (Passwords longer than 14 characters are preferred and can be simple as shown)
  - Simple letter substitution is not considered acceptable. (Example – Zeros, ones, and fours should not be used to replace "O"s, "I"s, or "A"s in a password. For instance "D1ct10n4ry" **is not** a secure password.)
- Users can access, use, or disclose electors' sensitive personal identifying information only when necessary to perform a job duty. These actions must be expressly authorized by designated County or State elections officials.
- Users may not display or provide electors' sensitive personal identifying information to unauthorized persons.
- Sanctioned SCORE system users must ensure proper workstation use. As responsible parties they must:
  - Only access SCORE on systems that are managed and controlled by the County or State. Users may not utilize a user-owned device to access SCORE.
  - Ensure electors' sensitive personal identifying information is not displayed on a computer screen so that unauthorized persons may view the sensitive information.
  - Ensure their screen is locked to prevent access to SCORE whenever they leave sight of a terminal.
  - Practice safe-surfing habits. A user may not casually browse the internet on a system utilized to access SCORE.

_____ **INITIALS**

SCORE
End User Acceptable Use Policy

- Not install or download any software including shareware, freeware, or browser controls unless authorized by County or State elections management staff to do so.
- Contact SCORE Customer Support immediately if a systems performance becomes erratic, or if it appears the system has been tampered with, or the local virus protection software finds an infection. Degraded system performance or erratic behavior may indicate a Malware infection such as a virus or Trojan.
- Only connect to county controlled networks with proper network security controls in place. A user may not connect to open or shared public-use networks.
    - If wireless networks are in use, they must at a minimum meet the following requirements:
        - WPA2 or above security enabled;
        - Shared wireless passwords/secrets must be changed every three months.
        - Wireless keys must be a minimum of 14 characters in length and meet complex password requirements. (See above)
    - All networks and systems must have proper security controls to ensure malicious users are not connecting to the network with the intent of intercepting SCORE communications or otherwise attacking SCORE systems.
        - The controls must include at a minimum network firewalls and securely configured network equipment to prevent common attack mechanisms.

- Failing to comply with this policy may result in the user's loss of access to the SCORE system, and could result in disciplinary action, and civil or criminal liability, or both under applicable provisions of federal and state law.

USER ACKNOWLEDGEMENT:

I certify that I have reviewed, understand, and agree to the SCORE End User Acceptable Use Policy. By signing this form, I affirm that I will abide by the SCORE End User Acceptable Use Policy, procedures, and guidelines. I have completed the SCORE Cyber Security training and am aware of what sensitive data is as well as best practices to protect sensitive data. I agree to treat all personal identifying information as sensitive, and will not disclose any elector's personal identifying information to anyone without the express permission of the Secretary of State or the County Clerk and Recorder. If I have any questions regarding this policy, I will obtain clarification from my supervisor before taking any action.

Name Printed: _____ County: _____

Signature: _____ Date: _____

_____ **INITIALS**