

Secure Elections in Taylor County

Security is s top priority for election professionals across the state of Florida. Here is a view as to what Taylor County is doing to ensure secure elections.

Voter Registration

- ✓ Voter registration applications are processed through the Department of State, Division of Elections, to verify the applicant meets state eligibility requirements, including identity and citizenship.
- ✓ The Department of State's online voter registration (OVR) website includes security measures to help ensure the identity of the voter is true and accurate while also protecting a voter's personal information. OVR requires a Florida driver license or state identification card number and the issue date, plus the last four of the social security number.
- ✓ Our voter registration database is updated routinely to remove deceased voters and felons per state statute and to identify and remove voters who have moved out of our county.

Voting

- ✓ To cast a ballot in Taylor County, a voter must be eligible and registered with a residential address in Taylor County.
- ✓ Voters must present a current and valid form of photo and signature identification to receive a ballot during early voting or on election day.
- ✓ If a voter registers by mail and has never voted in Florida, or has not been issued a Florida drivers license, Florida identification card, or Social Security number, they will be required to provide additional identification prior to voting the first time.
- ✓ For mail ballots to be counted, the voter must sign the return envelope that is provided, and the voter's signature must match the one they have on file with our office.
- ✓ Florida is a paper ballot state, leaving a trail for every vote cast.
- ✓ Once a voter checks in at the polls or their mail ballot has been accepted, their record is marked as voted. The voter will be flagged as "already voted" in the database and if they attempt to vote twice in the same election this flag will be displayed.

Tabulation and Tampering

- ✓ Our state-certified voting equipment is rigorously tested prior to each election with a public logic and accuracy test to verify the equipment will accurately count and record votes exactly as marked.
- ✓ Security seals are applied to all voting equipment and documented prior to deployment to assist election officials with the detection of possible tampering.
- ✓ Individual paper results are printed at each precinct and returned to our office on election night to verify a match against the electronic transmission.
- ✓ Precinct results are encrypted and electronically transmitted to a stand-alone server, that has no connection to the internet, to tabulate and report election results.
- ✓ Paper ballots are held and stored for 22 months after an election and can be used to verify results.
- ✓ A public manual audit is conducted after each election where ballots cast during early voting, vote by mail and on election day are hand-counted in a randomly selected precinct and race to ensure the machine count is equivalent to the human count.

Network Security

- ✓ We have purchased and are installing an ALBERT Sensor, which will be placed online before the Primary and General Election. This sensor will monitor our network 24/7 for any possible intrusion attempts or suspicious activity.
- ✓ We are running a highly rated virus software package; malware software package and we ensure all our desktops and servers are patched and up-to-date.
- ✓ We have joined the Multi-State Information Sharing and Analysis Center (MS-ISAC) and Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) and subscribe to their updates and newsletters.
- ✓ Department of Homeland Security has completed a physical inspection of our physical location and building to analyze the property and provide industry standard security protocols.
- ✓ We utilize an industry leading firewall solution that is updated, contains a list of blocked IPs and includes reporting tools to identify network security threats, issues and trends.
- ✓ Policies are in place for user passwords and use and security of office equipment.
- ✓ All employees have taken and passed a cyber security awareness course provided by the Florida Department of Law Enforcement (FDLE).