What Marion County Does to Secure Elections

Voter Registration

✓ Voter registration applications are processed through the Department of State 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 ID card number and the issue date, plus the last four of the social security number.

✓ We utilize a variety of reports and processes specific to Marion County to validate voter data.

✓ Our voter registration database is updated routinely to remove deceased voters and felons per state notification and to identify and remove voters who have moved per county and USPS notifications.

Voting

✓ To cast a ballot in Marion County, a voter must be eligible and registered with a residential address in Marion County and vote in their home precinct.

✓ Voters must present a current and valid form of photo and signature identification prior to receiving a ballot.

✓ 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 and will be flagged as "already voted" if they attempt to vote twice in the same election.

🔒 Tabulation and Tampering

✓ The Election Center is under 24-hour camera surveillance and doors are alarmed and monitored by a third-party security service and have restricted key card access.

✓ 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 examine, 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 copy.

✓ 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 under video surveillance for 22 months after an election and can be re-scanned or verified by hand should any disruption or corruption in the transmission of results occur.

✓ A public manual audit is conducted after each election where ballots are hand-counted in randomly selected precincts and races to ensure the machine count is equivalent to the human count.

🖥️ Network Security

✓ We purchased and installed an ALBERT Sensor, which was placed online in January of 2018.

✓ We are running a very highly rated virus software package (that has not submitted its source code for Russian review), a malware software package, and we ensure all our desktops and servers are patched and up-to-date.

✓ We have joined Multi-State Information Sharing and Analysis Center (MS-ISAC) and Election Infrastructure Information Sharing and Analysis Center (EI-ISAC), and subscribed to their newsletters.

✓ We have contacted The Department of Homeland Security (DHS) and MS-ISAC to do scans of our systems and to notify us of any known vulnerabilities.

✓ We utilize an industry leading firewall solution that is constantly updated, contains an ever-increasing list of blocked IPs', and includes a network security visibility solution that provides reporting tools to identify network security threats, issues and trends.

✓ We use an active directory weak password tester that checks for 10 different types of weak passwords.

✓ All employees have taken (and passed) a cyber security awareness course provided by the Florida Department of Law Enforcement (FDLE).

✓ Understanding that it's still the human that is the most vulnerable, we have purchased phishing education software that allows us to send phishing emails to our users, using the latest ploys or sometimes very targeted ploys.