ELECTIONS & INFORMATION TECHNOLOGY

ELECTIONS SECURITY

WHAT YOU NEED TO KNOW

Mono County prioritizes the safety and security of our employees, data, and electronic systems, particularly as it relates to elections. The Information Technology Department works closely with the Registrar of Voters and Mono County Elections Team to ensure that we are able to conduct safe, secure, and efficient elections where every vote counts. This information sheet is designed to provide a high-level overview of the work that goes into ensuring this takes place.

What is Mono County doing to secure elections?
Mono County follows industry standards and best practices to ensure that we have an effective security posture throughout the organization. This begins with ensuring that our PCs, servers, and other technology systems are up to date with the latest versions of software and patches and extends all the way to requiring all election staff (and all County personnel) to participate in monthly security awareness training.

How is Mono County keeping up on the latest security threats?
Mono County partners with and is supported by the Elections Instructure Information Sharing and Analysis Center (EI-ISAC) which shares critical information about threats and best practice responses with us on a regular basis. Furthermore, our security personnel are part of the Critical Infrastructure Protection Council under the Department of Homeland Security, as well the Elections Critical Infrastructure Governing Council.

What is Mono County doing to ensure that my vote will be counted and not deleted or changed?
Mono County is a leader in the State in terms of staffing as well deploying appropriate tools to protect our election infrastructure. We are one of a few counties across the Nation who deploy sensors supported by the DHS that help us monitor network traffic. Additionally, we conduct an annual security assessment based on the NIST Cyber Security Framework (NIST 800-53) which helps us shape and improve our security posture.

How is the County protected against Ransomware and similar Malware which could corrupt elections data?
Elections computers are separated from the internet and regular County network in order to ensure that they are not accessible to the outside world. This limits the number of people who have access to those computers and therefore reduces the risk of them becoming infected by Ransomware or Malware. Additionally, the County regularly backs these systems up to ensure that if they were ever infected the data could be recovered.

Is it true that the Russians hacked into other agencies in the Nation and changed elections results?
This is a false statement. No 'hacking' of elections infrastructure resulted in actual vote changes in the Nation. While five states' (and perhaps additional local agencies) election registration rolls were accessed by unauthorized users, it is important to understand that those rolls are public information and no registration roll databases were altered.

For a formal statement on Russian Elections Interference by the Department of Homeland Security, see https://www.dhs.gov/cisa/news/2019/07/25/joint-gcc-scc-statement-senate-intelligence-committees-first-russian

The Russians are using Social Media, like Facebook, to disrupt our elections and to vote for a specific candidate, right?
Not exactly. Russia (as well other nation states) have used, and continue to use, social media to disrupt political discussions, sow intraparty discord, and generally try to discourage voter turnout or suppress votes from certain demographics.

For more information please see https://www.dhs.gov/publication/foreign-interference and https://www.dhs.gov/news/2018/08/24/dhs-fbi-hold-joint-briefing-election-officials-facebook-and-microsoft