



Recommendations for Minimizing Cyber Risk

Political parties, candidates and elections administrators cannot be alone in the fight against malicious actors who seek to undermine our elections. As political campaigns and organizations are targets of cyber threats, they too have a role and responsibility in defending our democracy. **Your actions are critical in maintaining public trust in our elections** and minimizing the threat of cyber incidents.

As an integral part of protecting our democracy, I wish to remind you to **take preventative measures to reduce the likelihood and severity of cyber incidents.**

Recognized best practices for minimizing risk:

- (1) Establish an information security framework that allows your team to identify threats, create safeguards, detect incidents, respond quickly, and recover with resilience;
- (2) Control access to data and information systems; monitor vendors, contractors, and employees; and know what your users are doing with your data;
- (3) Beware of social engineering attempts, such as phishing emails, aimed at acquiring confidential or personal information from phone, email or other communications;
- (4) Educate your employees and volunteers on cybersecurity best practices, including how to recognize a phishing email, creating and maintaining strong passwords or passphrases, utilizing two-factor authentication, and avoiding dangerous applications;
- (5) Ensure your software and hardware security is up to date and properly configured;
- (6) Monitor user activity;
- (7) Back up your data;
- (8) Run regular security audits, assessments, and penetration testing; and
- (9) Monitor social media for false or misleading election information. Report such posts to social media platforms and the California Secretary of State's Office of Election Cybersecurity at cybersecurity.sos.ca.gov.

Other resources:

- Harvard Kennedy School's Belfer Center for Science and International Affairs published [The Cybersecurity Campaign Playbook](#) in 2018, which provides information and strategies for keeping campaigns secure.
- The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) provides services such as cybersecurity assessments, detection and prevention of threats, and information sharing and awareness. <https://www.dhs.gov/cisa/election-security>.
- The Global Cyber Alliance (GCA) offers several free toolkits to help election officials mitigate cyber risks. <https://gcatoolkit.org/elections/>.

If you detect suspicious activity:

In the event you observe or detect any suspicious activity, please alert law enforcement officials immediately and please contact my office with any important information. As a reminder, state law requires any entity that has access to voter data from the Secretary of State's office to report a breach of this information to our office as quickly as possible.

Should you have any questions or desire additional information, please feel free to contact Susan Lapsley of my office at (916) 695-1662 or slapsley@sos.ca.gov.

Sincerely,

California Secretary of State

