First Things First

Operational Security Fast Wins for Election Offices

FOR LOCAL ELECTION OFFICIALS AND SMALL TEAMS

IMPLEMENT THESE PRACTICES THIS MONTH

KEEP IT SIMPLE AND VERIFY AS YOU GO

ELECTION SECURITY *Exchange*

Operational security, or OpSec, is the practice of protecting sensitive information by controlling what we share, how we share it, and who can access it. In election administration, this does not just mean protecting ballots and equipment. It also includes reducing the exposure of small pieces of information that, when combined, could expose staff, facilities, schedules, or sensitive procedures. OpSec is about everyday habits, thinking ahead before speaking, posting, or publishing, and limiting references to details that are not legally required to be public.

For election officials, OpSec is not about hiding what you do, or even who you are. You can, and should, be proud of the way elections are administered and the integrity of the people and the systems involved. OpSec is about ensuring you are maintaining that integrity and taking the small steps necessary to make it harder for any bad actors intent on disrupting the process or targeting election officials.

Together, these principles point to a simple truth: strong OpSec comes from awareness, not secrecy. It's about recognizing where small details can accumulate into real vulnerabilities and taking practical steps to reduce the exposure. With that in mind, the following five areas highlight common OpSec risks and provide straightforward and easy ways to mitigate them.

1. Remove Public Staff Directories and Direct Contact Lists

The Risk

Publicly posted staff directories, direct phone numbers, and internal extensions enable targeting, phishing, harassment, and impersonation.

What to do

1. Remove full staff email and phone directories from your website.
2. Do not post printed staff directories at public counters.
3. Use general email inboxes and main office numbers instead of publishing individual direct lines.
4. Limit the information in email signatures to essential contact information.

Quick validation check

- Review your website and front counter materials.
- If a stranger can easily map your team structure and contact staff individually, reduce exposure.

2. Standardize Responses to Operational Questions

The Risk

Seemingly harmless procedural details can be combined into meaningful intelligence.

What to do

1. Develop short, approved responses for sensitive operational questions.
2. Train frontline staff to provide only information that is legally required to be made public.
3. Route detailed process questions to designated supervisors.

Quick validation check

- Ask a staff member an unscripted operational question such as how results are transmitted from polling places to the election office.
- If they provide specific storage locations, schedules, or security details beyond what is public, tighten the guidance.

3. Limit Routine and Travel Information Posted Online

The Risk

Public posts about travel, daily routines, and habits can expose patterns, physical absence from home or work, or predictable schedules.

What to do

1. Encourage staff not to post about travel, even personal travel, until after they return.
2. Avoid posting real time location updates, for example “I’m having a really great time at the county association conference here in Great County State Park”.

3 Disable geotagging on your smartphone so that no one can see where you are at any time.

4 Discourage repeated posts that reveal consistent routines, for example the same weekly coffee location or regular after-work patterns.

5 Review privacy settings on social media accounts. Your personal social media account should be restricted to just your friends and family.

Quick validation check

- Check your personal social media accounts to make sure your own posts are only being shared with friends and family.

4. Protect Information From Inappropriate Disclosure

The Risk

Observers, media, or visitors can capture sensitive details through casual photography or shoulder surfing.

What to do

1 Keep whiteboards and internal notes out of public view.

2 Use privacy screens for monitors in public facing areas and laptops used outside the office.

3 Position printers, check in sheets, and call logs away from counters.

4 Avoid looking at work-related documents in public spaces.

5 Keep work credentials and personal identification out of sight.

6 Place signs clearly designating “staff only” or “authorized personnel only” areas. Clear rules reduce confusion and risk and protect sensitive materials. These signs can help reinforce the idea that while there are boundaries, the process and activities are not being hidden. They also show that the same rules are applied consistently to everyone.

Quick validation check

- Stand in the public area and take a photo.
- Zoom in. If you can read private internal information, reposition materials.

5. Adjust Name Badge Practices

The Risk

Full names combined with visible credentials make it easier to identify, research, or target staff.

What to do

1. Unless legally required, use first name or last name only on badges.
2. Avoid listing full titles if not necessary.
3. At conferences or public events, remove badges immediately when leaving the event space.
4. Do not wear badges in restaurants, hotels, or during travel to and from events.

Quick validation check

- If someone saw a badge for five seconds, could they easily locate that staff member online? If so, reduce identifiable information.