First Things First

Quick Wins to Limit Risks of Insider Threats

ELECTION SECURITY *Exchange*

FOR LOCAL ELECTION OFFICIALS AND SMALL TEAMS

IMPLEMENT THESE PRACTICES THIS MONTH

KEEP IT SIMPLE AND VERIFY AS YOU GO

Improving your security posture by minimizing the risk from insider threats doesn't require deep technical expertise. It starts with a few simple, proactive habits.

What Is an Insider Threat?

Any person (current or former employee, contractor, vendor, volunteer, or partner) with authorized access who, intentionally or not, causes harm.

There are three types of insider threats:

UNINTENTIONAL

Accidents

- Mistaken uploads of sensitive information
- Lack of understanding about access or procedures

NEGLIGENT

Careless behavior

- Weak or reused passwords
- Unattended equipment or unlocked workstations
- Mishandled or misdirected data

MALICIOUS

Deliberate harm

- Theft, sabotage, or espionage
- Collusion with outside actors
- Intentional data exfiltration or destruction

QUICK WINS

1. Build a culture of reporting

Impact: High | Effort: Low | Time: 30 Minutes | Cost: Free

Why this matters:

Things are going to go wrong, and that is expected. If you build a culture of reporting, people will inform you when they've made a mistake or noticed something is off. This will help you identify insider threats that are unintentional or negligent. Additionally, when the culture is to continuously look for and report security issues (i.e., "See Something, Say Something" mentality), staff will inform you of situations that others may not have seen or reported.

When someone is making the same errors or is consistently trying to access systems or locations they should not, you may need to investigate. Some incidents may only call for additional training. But if someone has already been warned and trained on proper processes, repeated violations may be intentional. Further action, including firing and/or notifying law enforcement, may be necessary.

Building a culture of reporting requires a degree of understanding of unintentional errors. Highlight how the whole office benefits when people learn from mistakes and help prevent them in the future. A culture that relies on harsh reporting can create resentment and reduce the likelihood that people will report mistakes, including their own.

A clear reporting structure also needs to be established. Identify the appropriate reporting channels, including a supervisor and an alternative point of contact, when the supervisor may be involved in the issue. Having a representative of Human Resources or another person outside the hierarchy is a good practice.

2. Review, document, train on, and practice current SOPs

Impact: High **Effort: Low** **Time: 4-8 Hours** **Cost: Free**

Why this matters:

Standard operating procedures (SOPs) should guide staff work, ensuring consistent, repeatable steps and procedures that fit into the office's overall security posture.

Creating an SOP can feel intimidating because many people assume it has to be long and complex. It doesn't. A concise, one-page SOP can be just as effective. These should be written down and provided to staff regularly or be easily accessible. It's critical to review them each election cycle. Like building a reporting culture, SOPs also drive the behavior of your team. They also provide 'protective' and 'detective' security measures. When staff are trained to follow proper procedures, it helps protect against negligent and unintentional insider threats. It also allows you to detect deviations from expected practices, which may lead to additional training or investigation. Start with your highest-risk SOPs, such as access protocols for the voter registration system or ballot storage location(s). Defining potential threats at the top of an SOP can help staff recognize the concerns and the importance of following procedures.

3. Review access logs for critical systems and storage locations

Impact: High **Effort: Low** **Time: < 30 Minutes** **Cost: Free**

Why this matters:

Elections face insider threat risks like any industry. Effective access control requires knowing exactly who can reach sensitive systems and data. Election workforces shift every cycle, bringing in temporary staff, volunteers, vendors, and personnel from multiple agencies, often with limited time for vetting. Many of these workers have access to sensitive systems. Any access lapse can undermine public trust in the election process.

Reviewing access logs is an important security measure. You might uncover gaps or suspicious activity. Equally important, you're establishing a culture of accountability and signaling to your team that the security measures you require them to take are meaningful and serious. And anyone acting in bad faith will know they are likely to be caught.

Logs can be digital if you have swipe card access, analog, like a paper logbook, or both. Knowing how to access the logs means you'll be able to act quickly if you need to investigate something.

As you review logs and related materials, put yourself in two roles. First, think like an outsider – someone without visibility into your security controls, who isn't yet convinced that access is well-managed. What gaps in your logs or documentation might leave that impression? Are there ways your current records fail to clearly show that access is limited and monitored? Adjusting your policies and documentation to close those gaps doesn't just tighten security, it also builds confidence in your controls.

Second, think like an adversary – a nefarious insider looking for ways to exploit weaknesses. Are there gaps that they might exploit, or may have already exploited? Do you see log-in times that don't make sense, or log-ins by people who don't or shouldn't have access? Or a single sign-in for people accessing a room or ballots as a pair or team?

Every employee needs checks and balances placed on them, including leaders. Even well-intentioned people can be moved to act outside their authority - sometimes without realizing it, and sometimes convinced they're doing exactly the right thing. Access controls, such as only handling sensitive materials when someone else is present, protect everyone from speculation and criticism.

Do it!

- Start documenting who has access to each area or system, along with the types of data stored there and the level of impact associated with that access.
- If too many people have access to an area or system, make modifications.
- Where too much access is given to an individual, reduce their access to only what they need to do their job successfully.
- Increase oversight and detection mechanisms, such as supervision, logging, seals, cameras, etc.
- Set a calendar reminder to review one log every month.

4. Add insider threat awareness training to annual staff and volunteer onboarding

Impact: High **Effort: Low** **Time: < 15 Minutes** **Cost: Low/Free**

Why this matters:

Identifying and responding to insider threats is a team effort. Regular training gives every staff member the knowledge to recognize and report warning signs, multiplying the eyes and ears watching for problems across your entire office.

The good news: election administration already has a built-in security culture. Bipartisan teams, two-person rules, chain of custody procedures, and public observation rights all exist precisely because elections are designed to be verified by multiple sets of eyes. Security awareness training is not a new concept, rather it is an extension of what election officials already do every day.

Do it!

- Add a brief "dos and don'ts" security awareness module to your existing onboarding for all staff and volunteers. Even a 10-minute overview can be very helpful.
- Frame the training around familiar election norms: bipartisan teams, two-person rules, chain of custody, and public accountability.
- Clearly explain what "unusual activity" looks like and who to report it to.
- Reinforce that reporting is expected, professional, and consistent with how elections have always worked.
- Identify a reporting contact who is outside the direct chain of command so staff feel safe coming forward regardless of who is involved.

5. Conduct a tabletop scenario with staff

Impact: High **Effort: Low** **Time: 1 hour** **Cost: Free**

Why this matters:

Taking time to consider the risk from insider threats keeps the issue top of mind. An exercise can be as simple as running through the following scenarios:

SCENARIO 01

A long-serving poll worker tells a colleague that the voting machines are "connected to the internet" and they are going to "break the seals to take pictures of the inside of the machine."

DISCUSSION QUESTIONS:

1. Does this person currently pose an insider threat, or are they expressing concern? What is the difference?
2. What category of insider threat does this represent: unintentional, negligent, or malicious?
3. At what point does expressing a belief become an actionable threat?
4. Who in your office would you talk to about this, and what would you expect them to do?

SCENARIO 02

A county clerk receives an anonymous tip that a deputy clerk has been photographing proprietary and confidential information and sending it to an unknown contact. The deputy clerk is also a candidate in an upcoming local race.

DISCUSSION QUESTIONS:

1. Is this an emergency or non-emergency situation at this stage? What is the threshold for emergency intervention?
2. Who needs to be contacted first: HR, the county attorney, law enforcement, or your state election authority?
3. How do you restrict access without tipping off the person or contaminating potential evidence?
4. How would you communicate with the rest of your staff during an active investigation to maintain trust without disclosing details?

SCENARIO 03

A staffer tells you she is surprised that a co-worker was calling a precinct late on Election Day and reading off the names of about 30 voters, confirming those voters had not voted by mail or during early voting. She couldn't figure out what the purpose of the call was. She was concerned that a poll worker might be casting ballots in these names.

DISCUSSION QUESTIONS:

1. Are there legitimate reasons a staffer might confirm the vote-cast status of a large number of voters late on election day?
2. How might a poll worker in a precinct use this information?
3. How would you investigate? Do reconciliation forms or signature books offer information that could prove all voters in the precinct were legitimate, or flag any that may not be?

Insider threat mitigation is not about perfection; it's about steady, repeatable habits that strengthen trust and protect the office. By building a reporting culture, maintaining clear procedures, reviewing access permissions, and training staff, you create an environment where problems surface early and everyone knows their role. Small, consistent actions taken now will reduce risks throughout every election cycle.