acet
AMERICAN COUNCIL FOR ELECTION TECHNOLOGY

Election Technology Access Risks

Best Practices for Managing External Pressure and Insider Overreach

TWO THREATS EVERY ELECTION OFFICE FACES

EXTERNAL PRESSURE

People outside your office demanding access to election technology, systems, or facilities, often claiming authority or urgency.

INSIDER OVERREACH

People who already have legitimate access but exceed, misuse, or abuse that access.

IF YOU'RE FACING EXTERNAL PRESSURE

REMEMBER THESE **3 THINGS**

PAUSE AND VERIFY

"Let me confirm this through official channels."

Legitimate officials, attorneys, vendors, and law enforcement will wait. **Legitimacy is patient.**

Urgency is **not** proof of legitimacy.

LOG THE INTERACTION

On a clipboard form or intake log, record:

- Name
- Organization
- Purpose of request
- Date & time
- Contact information

FOLLOW YOUR CHAIN OF COMMAND

At a minimum CoC should involve:

- Your supervisor
- Legal counsel

Do **not** let someone else's urgency override your protocol.

IF YOU SUSPECT INSIDER OVERREACH

REMEMBER THESE **2 THINGS**

DOCUMENT OBSERVED BEHAVIOR

Create a contemporaneous memo:

- Exact statements made
- Actions observed
- Dates and times

Write it the same day in a notebook or individual typed documents.

Stick to observable facts not opinions.

ENGAGE LEGAL COUNSEL AND HR

Do **not** confront the individual first.

Let counsel guide next steps and preservation of evidence.

This resource shares best practices only. It does not constitute legal advice and does not create an attorney-client relationship.

Info@TechForElections.VOTE acet

Election Technology Access Risks

KNOW YOUR JURISDICTION'S ELECTION TECH PROTECTIONS

Criminal protections for election technology vary widely by state and jurisdiction. ACET recently completed a 50-state survey examining statutory protections for election technology tampering. ACET published the statutory language, links to official laws, and the penalty for violating these statutes at TechForElections.VOTE/resources to give you a baseline understanding of where your state is situated. But you should have guidance on your specific circumstances and jurisdiction, so, ask your jurisdictional (municipal, county, state) attorney for a briefing.

REQUEST A BRIEFING FROM YOUR JURISDICTIONAL ATTORNEY

Use these questions to understand the outward legal contours **before** a crisis:

1. ***What election technologies are covered by criminal tampering statutes in our jurisdiction?***
2. ***How are those technologies defined?***
3. ***Does our statute protect just the data, or also the software, system, and/or physical equipment?***
4. ***Do those statutes cover all personnel in my office? Or only specific people?***
5. ***What are my rights to refuse outside access requests?***
6. ***What are my obligations when someone demands access? i.e., when must I comply?***
7. ***Is the attempt itself criminal, or only successful tampering?***

TEMPLATE CARD

Laminate and put it at every desk where someone might receive an access request.

CHAIN OF COMMAND

1. _____
2. _____
3. _____

LEGAL COUNSEL CONTACT

Name: _____

Phone: _____

OFFICIAL VENDOR CONTACTS

Vendor: _____ Phone: _____

Vendor: _____ Phone: _____

REMEMBER: **LEGITIMACY IS PATIENT.**