First Things First

Physical 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*

Physical security doesn't require high costs or specialized infrastructure. Small, intentional steps can make a measurable difference. Security works in layers, and no single layer can stand on its own. For every protective measure that deters or slows unauthorized access, there must be a corresponding detective measure that alerts you when something isn't right. Layering protection with detection creates a stronger, more aware environment. These five low-cost, high-impact actions help prevent problems, surface issues early, and build the daily security habits that keep your office resilient.

1) Control Access to Your Building

Impact: Very High **Effort: Low** **Cost: $–$$$**

Why this matters

Access control is the backbone of physical security. Protective measures such as strong locks, restricted areas, clear entry procedures and secured doors reduce the chance that someone can enter without authorization. However, any protective layer can be bypassed or fail. Detective measures, such as alarms, visible badges, access logs and simple alert systems, can help catch problems early.

When budgets allow, electronic access control systems (cards, fobs, phone apps, or keypads with audit trails) provide a much higher level of protection. Badges help with visibility, but they don't stop unauthorized entry. True risk reduction comes from real access control: systems that enforce who can enter and that create an auditable record of every access event.

In most real-world breaches, the failure isn't high-tech—it's a door left open, unclear rules, a missing key audit or not having a way to detect who entered a space. Tightening access points and pairing protective measures with detective tools dramatically reduces opportunistic threats and gives staff immediate awareness when something isn't right.

Do it!

- Upgrade all exterior doors with commercial deadbolts
  - » Defiant Single Cylinder Deadbolt ($12)
  - » Kwikset Deadbolt ($20)
- Add padlocks to interior storage rooms
  - » Stainless Steel Discus Padlock ($13)
- Install door alarms on secondary entrances
  - » GE Personal Door Alarm ($21)
- Install Video Intercom, Door Release System
  - » Adrinfly Wired Video Intercom System 7"
  - » Vrbgify 2-Way Video Unlocking System 7"
  - » AMOCAM Wired Video Intercom Unlocking System 7"

- Add “Authorized Personnel Only” signage (in-house printed) to all restricted spaces, including ballot rooms, equipment storage areas, staff-only corridors, tabulator rooms, and any interior door where public access should stop
- Electronic Access Control
  - » Ultraloq Latch 5 Series
  - » Yale Assure Lock 2
- Issue badges to staff and visitors ($26)
  - » Staples ID Badge Holders with Lanyard
- Post clear rules at the entrance in line with what is allowed in your jurisdiction
  - » “No recording beyond this point” or “All visitors must sign in and be escorted.”
- Maintain an access log
  - » Log every visitor, vendor, or delivery entering restricted areas—even a simple notebook works.
  - » Record name, time in/out, who escorted them, and purpose.
- Escort all non-staff within the building
- Set up a staff “code word” alert system
  - » A no-cost option when panic buttons aren’t available.
  - » Use a pre-agreed phrase that signals there is a problem that requires immediate action.
  - » Train all staff, including poll workers, on how it is used.
  - » Keep it simple, discreet and practiced.
- Audit physical keys and electronic access badges
  - » Maintain a master list of every key and badge issued.
  - » Verify who has them; whether any are missing, outdated, or unreturned; and immediately deactivate lost or inactive credentials.
  - » A quarterly audit helps catch gaps before they turn into unauthorized access.

Quick check: Walk the building at random. All unused doors should be locked. No propped-open doors. All staff should have a visible badge. Verify access logs are present and used.

2) Improve Indoor & Outdoor Visibility of Election Facilities and Ballot Boxes (Lighting + Cameras)

Impact: High **Effort: Low** **Cost: $–$$**

Why this matters

Visibility is one of the most effective low-cost security tools. Protective measures like lighting and mirrors make it harder for someone to conceal themselves or tamper with a ballot box or equipment. Detective measures like cameras, monitored video doorbells and motion alerts help you see when something unusual happens and respond quickly.

Visibility fails when cameras are installed and never checked. Too many offices discover issues days or weeks later – after footage is overwritten or deleted. Cameras only provide security if you monitor alerts, review footage and assign responsibility for checking them.

Do it!

- Add low-cost indoor/outdoor cameras
  - » Blink Outdoor ($51)
  - » Wyze Cam v4 ($35)
  - » Blink Mini Indoor ($29):
- Add monitored video doorbells
  - » Ring Wired Doorbell
  - » Ring Floodlight Cam Plus
  - » Ring Business Solutions for Monitoring
- Use solar-powered exterior lighting around the building and parking lots
  - » Solar Motion Sensor Outdoor Lights ($13)
- Install convex mirrors to remove hallway blind spots
  - » IC1800 18” Acrylic Convex Mirror, 18 Inch

Quick Check: Do an after-hours walk-through with the lights off. Spots that feel hidden, shadowed, or outside the camera’s view are red flags—add lighting, a camera or a mirror to eliminate them. Check that cameras are functioning, pointed properly, sending alerts, and retaining footage. A blind spot you notice now is a blind spot a threat actor can exploit later.

3) Harden the Perimeter and Control Access Points (Planters, Barriers, Signage)

Impact: Medium–High **Effort: Low** **Cost: $–$$**

Why this matters

A building's exterior is the first line of defense. Protective measures – planters, bollards, standoff barriers and intentional landscaping – create distance between the public and your entrance, discourage vehicle approach, and reduce places where someone can hide or linger. Detective measures like marked boundaries, clear visibility lines, and controlled pathways make it easier to notice when someone enters a restricted space or behaves suspiciously.

Thoughtful landscaping is especially important. Overgrown shrubs, tall grasses or dense vegetation can create concealment spots and compromise camera visibility. When maintained strategically, landscaping supports good sightlines, increases natural surveillance and reinforces access-control design.

Do it!

- Use large planters as bollards ($500)
  - » Grainger Planter Bollard
- Add portable stanchions/rope barriers ($39)
  - » Roadhero Plastic Stanchion Post/Rope
- Use portable steel crowd-control barriers for high-traffic days ($50–$65)
  - » Industrial Expandable Metal Barricade 17 ft
- Mark "Public Area Ends Here" boundaries with floor tape or clean signage (free–$10)
- Add "No Unattended Visitors," "Entrance →" directional signage
- Maintain clear, security-focused landscaping
  - » Trim bushes and shrubs to 3 feet or lower to eliminate hiding spots
  - » Keep tree canopies trimmed up to 7 feet for clear visibility
  - » Remove dense or decorative vegetation that blocks cameras or creates blind areas near windows, doors, ballot boxes or pathways
  - » Use low-profile plants or gravel beds near entrances to deter loitering and maintain clean sightlines

Quick check: Stand at your main entrance and assess like an adversary.

- Could a vehicle approach within 5-10 feet of the door?
- Could someone hide behind landscaping, a planter, or a column without being seen?
- Could a crowd gather unimpeded at the door?
- Are the boundaries of public vs. restricted space obvious?
- Are cameras fully able to see the standoff area and landscaping?

If you answer yes to any of these, add barriers, adjust landscaping, or reposition cameras.

4) Secure Ballots & Sensitive Areas

Impact: Very High **Effort: Medium** **Cost: $–$$**

Why this matters

Ballots, USBs, memory cards, tabulators, and equipment rooms are the most targeted—and most consequential—assets in any election office. Protective measures like locked rooms, secure cabinets, and access restrictions prevent unauthorized handling and preserve chain of custody. Detective measures - tamper seals, access logs, key tracking, and surveillance - help you identify when something has been accessed, altered, or mishandled.

Just as important, no one should ever be in a highly sensitive area alone. A two-person integrity rule, modeled after bipartisan review teams, reduces insider-threat risk and provides built-in oversight.

Strong control over sensitive areas isn't just best practice, it's essential to maintaining public trust. A single unsecured door or missing USB drive can compromise confidence even if no harm occurs.

Do it!

- Add lockable steel storage cabinets ($150–$250)
- Use tamper-evident seals ($10–$20 per pack)
- Use laptop/USB locking cables ($15)
  - » Universal 3-in-1 Keyed Laptop Lock
- Add internal key management lockboxes ($30)
  - » KYODOLED Locking Key Cabinet

Quick check: Attempt to enter a sensitive room as if you were testing the system.

- Can you open the door without a key, badge or staff escort?
- Can you reach ballots, USBs or memory cards without breaking a seal or unlocking something?
- Would anyone know you entered—today or last week?
- Could one person enter alone without violating a rule?

If the answer to any of these is yes, you have a security gap.

5) Conduct a 10-Minute "Security Audit" Every Month

Impact: Medium **Effort: Low** **Cost: $0**

Why this matters

Threats evolve, routines drift and small vulnerabilities accumulate over time. A short, consistent audit keeps your protective measures tight and ensures detective measures are still working. This is how to catch problems before an adversary does.

Security is never "set it and forget it." Even simple issues – an unlocked door, a blocked camera, a dead light, a missing key – can undermine layers of protection. A monthly audit reinforces daily habits, builds staff awareness and ensures the environment stays resilient as operations change.

Do it!

- Walk the perimeter and check doors, lights, cameras
- Ensure storage rooms are locked
- Look for propped doors or blocked safety exits
- Test one camera feed weekly
- Confirm staff know who is "lead" for emergencies that day
- Ensure a clean desk policy
- Create a monthly calendar invitation for staff to complete this review

Quick check: Each audit should be documented, including any gaps identified and mitigations implemented.

- Assign someone to conduct the audit
- Create and follow an audit checklist
- Audit at least monthly
- Review past audits.
- Document issues/gaps
- Escalate issues
- Retain documentation

Reference Materials (Recommended Tools from CISA):

CISA publishes two easy-to-use checklists that can help structure or enhance your physical security. These are practical, election-specific tools built for quick reviews:

CISA Physical Security Checklist for Election Offices
A comprehensive, office-focused checklist covering access control, secure storage, visibility, physical barriers, and facility procedures.

CISA Physical Security Checklist for Polling Locations
A streamlined checklist designed for temporary, shared, or high-traffic locations such as polling sites, vote centers, and drop-box areas.

These checklists reinforce the layered security approach and help ensure you're not overlooking critical steps.

Disclaimer: The products referenced or linked within this document are presented solely for illustrative purposes. They do not constitute an exhaustive listing of available options, nor are they intended to be a commercial endorsement or recommendation.