CHAPTER 3: SECURITY[1]

Section 3.01 Election and Board Security Overview

This chapter discusses how to keep elections secure. It covers both physical and information technology (IT) security. It also covers how to keep the board office, equipment, and computer systems safe. It also includes what to do if something goes wrong. These rules protect elections and help voters trust the process.

This chapter is supported by Directive 2026-20 – *Security of Critical Infrastructure at Ohio's Boards of Elections,* 2026-20 *Security Directive Technical Document*, the 2026-20 *Security Directive Guidebook*, and the 2026-20 *Security Directive Checklist*.

Section 3.02 Security of the Board Office, Voting Systems, and Ballots

SECURITY OF THE BOARD OFFICE

Keeping the board office secure is crucial to protect staff, voting equipment, and IT systems. This helps ensure that elections remain confidential and trustworthy. The board must do its best to prevent unauthorized access and minimize risks such as damage from fire or water.

Board offices must have exterior lighting focused on entrances, exits, and the external drop box. This lighting should be inspected regularly to ensure it works properly.

Each location must also have adequate fire suppression equipment that is regularly checked to ensure it functions correctly. Portable fire extinguishers should be visually inspected every month for physical damage, such as corrosion, leaks, or dents, and to make sure the pressure gauge is in the correct operating range.

[1] Directive 2026-30

Boards must also have approved video monitoring systems for both the interior bipartisan rooms and the exterior drop box. These systems should keep footage for at least 14 days and be checked regularly to ensure they are working as expected.

Each board must create an office security policy that covers, at a minimum:

- How to keep unauthorized people out of the board office.
- How staff will register and monitor visitors.
- How to restrict access to areas that have voting equipment, election materials, voter registration servers, networks, and computers.
- How to check that people are following security rules.
- How to report if someone breaks the rules.

Review the board's security policies and procedures every six months to make sure they are current and being followed.

STORAGE OF VOTING EQUIPMENT

The board must use the following rules for storing voting equipment at the board office or other secure place:

- Store it in a secure, clean, and climate-controlled area.
- The voting equipment must be secured at all times. Access must be limited to as few board employees as possible, and video monitoring should cover the entrance and exit to the bipartisan storage areas.
- Equipment storage rooms must have alarms that detect if someone enters without permission.
- If a security alarm goes off, the director and deputy director must be notified. They must tell the Secretary of State's office through the Security Event email box.
- Use a dual-control lock system that requires a bipartisan team to unlock. The director (or designee from their party) must keep possession of one key or lock combination, and the deputy director (or designee from their party) must keep the other one.

- Check ID before letting any visitor, vendor, or repair person into equipment storage areas. Keep a log of the names and when they enter and leave. Watch visitors at all times. The best systems (badges or video monitoring systems) track exactly who enters and log the date and time of access.
- Install smoke alarms and fire extinguishers. Train staff on what to do if a fire occurs in the storage area.
- Follow the manufacturer's storage guidelines for voting equipment. Storing equipment improperly may affect its warranty.
- Keep the storage area clean. Do not store equipment in damp areas or on floors that might flood.

TAKING VOTING EQUIPMENT OFF-SITE

Sometimes, boards take voting equipment off-site for demos, public events, or because of an emergency.

Bipartisan control must be maintained at all times, even during transport and demos, unless the board hires a private delivery company. Follow rules from **Chapter 9, Section 3**, of this manual, including using tamper-evident seals. If a bipartisan team member must leave, a qualified person of the same party must step in.

Keep records in the board inventory control process of who has the equipment and when.

INVENTORY OF VOTING EQUIPMENT

The board must inventory all its voting equipment and keep a list of each piece and its serial number. For each piece of equipment, also keep:

- Proof of purchase (invoice, purchase order, etc.).
- Chain of Custody Log for at least two years after each election.[2]
- Usage records (when, where, and who used it).
- Reports of any damage or mishandling.
- Any repair records (when, where, who did the repair, reason, and outcome).

[2] See County Board of Elections Record Retention Schedule.

The director and deputy director must maintain and check the list often.

SECURE STORAGE OF BALLOTS AND ELECTION DATA MEDIA

Ballots and election data media include:

- Optical scan ballots made by a vendor or printed in-house.
- Blank ballot paper.
- Spoiled and/or unused ballots.
- All removable media cards.
- CDs or USB drives with results.
- Paper vote records, also known as voter-verified paper audit trails (VVPATs).
- Ballot access devices (such as Personal Electronic Ballot cartridges or access cards).

Store these materials in a clean, climate-controlled room that has proper smoke alarms and fire extinguishers. Don't store them in areas that may flood or get wet. No food or drinks are allowed in storage areas.

Only authorized staff may access these items. Keep them in a separate, locked room or storage unit that is for that purpose. Just like the voting equipment, ballots and election data media must be locked under a dual-control system.

Store ballots as the printer recommends or follow manufacturer recommendations for blank ballot stock. Use protective cases, containers, or original packaging if that is what the printer or manufacturer recommends.

Put removable media in a labeled sleeve or case.

INVENTORY OF BALLOTS

For outside-printed ballots:

- Boards must keep a list of the ballot styles and the number of ballots for each style that they get from the printer.
- Keep track of any difference between what was ordered and what was received. Show any steps board employees took to fix the problem.

- The board must maintain a list of each of the following:
  - The sequence numbers of the ballots received.
  - The number and sequence number range of the ballots given to each precinct.
  - The number and sequence number range of the ballots for absentee and provisional voting.

The board must document what happened to each ballot (voted, unvoted, or spoiled).

For ballots printed in-house with a ballot-on-demand (BOD) printer, the board must document the use of each sheet of blank ballot stock.[3]

Use a Chain of Custody Log to track the delivery of optical scan ballots to each precinct.

SECURITY OF VOTING SYSTEM AND TABULATION PROGRAMS/SOFTWARE

Ohio law states that voting machines must never be connected to the internet[4]. This includes all equipment and software used to set up elections, create ballots, collect data and count votes, tabulate results, and keep audit records. The board's voter registration server is not considered part of the voting system for this section.

Boards are prohibited from connecting the following devices to the internet: voting machines, marking devices, tabulating equipment, direct recording electronic (DRE) voting machines, election management systems, and central tabulating systems.

Voting machines or parts of the system must only connect to the central tabulating system through an air-gapped network for things like uploading memory cards, ballot definitions, and precinct results. Never download or install software or firmware on voting machines that has not been approved by the Board of Voting Systems Examiners (BVSE).

DAILY BACKUPS

Boards must back up the voter registration server and any data it processes every day. Other important systems, such as file servers, must be backed up at least once a week.

[3]No board of elections shall use a ballot-on-demand system unless each ballot printed by the system includes a tracking number. R.C. 3506.20(B).
[4] R.C.3506.23

These backups must be stored securely at an off-site, off-network location. Boards must keep backup copies for at least three weeks. At least once a year, boards need to test the backups to make sure they can fully restore the voter registration server and other critical systems using the off-site backup.

PASSWORDS

The board and its employees must use strong passwords. Set a basic input/output system (BIOS) password for all vote tabulation server systems. This forces users to enter the correct BIOS password to boot the machine.

All central tabulating systems must have passwords that:

- Are split between parties (a board employee from the Republican Party has half of the password, and a board employee from the Democratic Party has the other half of the password).
- Are at least 15 characters long or the minimum number that the system will allow, whichever is greater.
- Include a number in each half.
- Include a symbol in each half.
- Include both uppercase and lowercase letters in each half.
- Do not repeat the same character more than twice in a row.
- Do not use simple letter substitution (for example, "D1ct10n4ry").

How do split passwords work?

A split password has two separate 15-character passwords.

The employee representing the Republican Party knows one of them, and the employee from the Democratic Party knows the other.

Each employee enters his or her password without the other employee observing them enter it.

The voting system vendor may set these up for the board.

Some voting systems have bipartisan controls, with two separate passwords entered in separate boxes or on separate screens.

Change both the BIOS and central tabulating system software passwords before every election.

Only authorized users can have passwords for the BIOS and central tabulating system. Never put any part of a password on a monitor or keyboard or anywhere it can be seen.

Set systems to log out users after five minutes of no activity.

USER ACCOUNT MANAGEMENT

For all systems with voter information and central tabulating systems, every user must have their own user ID and personal password.

Require these IDs and passwords for multiuser access to computers and networks.

All users of board systems, email, and official social media must:

- Have a unique username and password/passphrase.
- Never share passwords or security devices.
- Use strong passwords that:
  - Are at least 15 characters long.
  - Contain three out of the following four items: number, lowercase letter, uppercase letter, and a symbol.
  - Doesn't contain the user's name or username.
  - Aren't simple dictionary words.
  - Aren't simple letter swaps (like "D1ct10n4ry").
- Use different passwords for different systems. For example, the passwords for personal email accounts and board of elections email accounts cannot match.

More Password Tips:

Avoid common or easily guessed passwords like these:

12345
12345678
password
iloveyou

To create a strong password:

Longer is better.

Use uppercase, lowercase, and numbers.

Use a passphrase like Thebestpartofthedayiswhenltakemy1stsipofcoffee.

- Passwords/passphrases must be encrypted while stored in a format prescribed under the National Institute of Standards and Technology (NIST) 800-53 5.1.1.2.[5]
- Change user passwords every 90 days and do not reuse passwords.

Password Tip

Using multifactor authentication (MFA) reduces the need to change passwords frequently.

Multifactor authentication must be used for all accounts that access voter data, election systems, email, admin access, or remote connections. Any multifactor solution must follow government standards (found in NIST 800-63b), by using hardware authentication devices, one-time use password tokens, or biometrics.

Boards using social media accounts must use multifactor authentication.

The board must review user accounts quarterly, remove access for people who don't need it, and deactivate unneeded accounts.

ADMINISTRATIVE ACCOUNTS

Administrative accounts can install updates, manage user accounts, and change system settings. After each quarterly review, determine everyone who has an administrative account and remove accounts that aren't needed.

Administrative accounts must be separate from accounts used for email, internet, and voter registration processing. Work with board IT staff to make sure employees with admin accounts only have access to systems needed for their role.

ALL OTHER PASSWORD GUIDANCE

For all other guidance on password creation and management, refer to the most recent Secretary of State *Security of Critical Infrastructure Security Directive*.

ACCESS LOGS

Directors and deputy directors must regularly check access logs kept by their voting system servers, voter registration servers, computers, firewall, and networking devices. Look for any strange activity on the system, such as access at odd hours or too frequently.

[5] SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations | CSRC.

For security, keep these logs on a separate system if possible. Save all access logs for 90 days. Electronic logs must not be turned off.

THIRD-PARTY PERSONNEL ACCESS TO VOTING SYSTEM

Board policies must prohibit anyone who is not a board employee, contractor, or consultant of the board or the Secretary of State's office from accessing election systems or networks without written approval from both the board chairperson and the director.

Remote access to board systems must use secure technologies (such as TLS v1.2+ or IPSEC) with multifactor authentication. Remote access must:

- Use VPN with multifactor authentication.
- Meet federal security standards (NIST FIPS 140-2 standards).
- Log and store all access sessions as required.

Before giving outside parties access, get written documentation that shows what work they'll do, who authorized it, who's responsible, and exactly when access starts and ends.

Section 3.03 Information Technology Security

TECHNICAL POINT OF CONTACT

Each board of elections must designate a Technical Point of Contact (TPOC). This TPOC can be an employee of the board of elections or an employee of an external IT support organization if the board contracts for such services, either through the county or a third party. The board is required to notify the Secretary of State's office whenever there is a change in the TPOC, including any updates to the TPOC's contact information.

CONNECTED SYSTEMS

All connected systems, including voter registration servers, computers, and network equipment, must follow the *Security of Critical Infrastructure Security Directive* that is sent directly to the board from the Ohio Secretary of State's office. This document is for official use only and is covered by R.C. 149.433.

VULNERABILITY MANAGEMENT

Boards must run weekly authenticated vulnerability scans and keep records on this for at least one year. Fix security problems quickly: Critical and/or high vulnerabilities must be

fixed within 15 days and others within 30 days. Using a patch management solution can help meet these deadlines.

EMAIL AND WEBSITE SECURITY

All board email addresses and websites must use domains ending in ".gov". Board members, directors, deputies, and staff may not use personal email providers (Gmail, Yahoo, etc.) for official business.

Never forward email messages to personal accounts (such as Gmail or Yahoo).

Boards must use email security tools (SPF (Sender Policy Framework), Domain-based Message Authentication, Reporting and Conformance, or DMARC, with DomainKeys Identified Mail known as DKIM) to prevent email scams and phishing. Learn more at: https://www.cisa.gov/eviction-strategies-tool/info-countermeasures/CM0055

All county board of elections email accounts must use multifactor authentication, and each permanent employee or member requiring an email must have their own email address.

NETWORK SECURITY

Boards of elections must set up their networks securely, as shown in the *Security of Critical Infrastructure Security Directive*. This document is for official use only and is exempt from public disclosure under R.C. 149.433. It adds to the rules of this section.

VOTER REGISTRATION AND ELECTION MANAGEMENT SYSTEM DATA

Areas with voter registration systems, election management systems, vote tabulation systems, pollbooks, electronic pollbooks, ballots, or other election systems must be secured. This security must use a two-person access mechanism, ensuring that access requires a bipartisan team.

Boards must back up the voter registration server and data every day. Encrypt these backups using federal security standards (NIST FIPS 140-3) as explained in the *Security of Critical Infrastructure Directive*. Store all backups in a secure, off-site location not connected to the board network. Test the backup once a year to make sure the board can fully restore the voter registration server if needed.

Section 3.04 Security

Election officials are responsible for protecting Ohio's elections. Each county board of elections must follow the steps in this section to strengthen security and protect IT systems.

THE MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER (MS-ISAC) AND CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) RESOURCES

The Department of Homeland Security (DHS) designated election infrastructure as critical, which gives election officials access to some free DHS services. For more information, contact DHS at CISAServiceDesk@CISA.DHS.gov.

Boards must continue using the Cyber Hygiene Vulnerability Scanning Service, which scans internet systems for security issues and tells users about these risks so they can fix them. Boards must continue to use the Web Application Scanning service, which scans the board's websites for vulnerabilities.[6]

Every two years, boards must request these DHS CISA services:

- Risk and Vulnerability Assessment: An on-site assessment that finds network security vulnerabilities and gives the board a report and recommendations.
- Remote Penetration Testing: Remote testing that identifies vulnerabilities in external systems, with a report and recommendations.

Boards must also update personnel information with the MS-ISAC and register new staff at Learn.CISecurity.org/MS-ISAC-Registration.

SECURING ONLINE CAPABILITIES

TLS/SSL certificates (digital certificates standing for Transport Layer Security and Secure Sockets Layer) secure data and prevent websites from being flagged as insecure. Each board must use these certificates for all web applications and make sure they don't expire.

[6]CISA defines a vulnerability as a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exploited, either accidentally or intentionally, leading to a security breach or violation of the system's security policy. Essentially, it's a potential weakness that an attacker could use to compromise a system.

All board websites, including vendor systems for election and voter data, must have a web application firewall (WAF). The *Security Directive Implementation Guidebook* provides more information on WAFs.

The board's WAF must include:

- Protection from denial-of-service attacks.
- Blocking of harmful scanning and bots.
- Defense against common web attacks (like cross-site scripting or SQL injection).

Boards must also show a banner on their website telling visitors how to check that the site is secure and official.

INCIDENT RESPONSE PLANNING AND PRACTICE WITH TABLETOP EXERCISE (TTX)

Boards must have a plan for handling security problems such as ransomware, phishing, and insider threats. The board must practice this plan once a year through a tabletop exercise (TTX). Boards must send updated Incident Response and Continuity of Operations Plans to the Secretary of State's Elections Division at Election@OhioSoS.gov.

Boards should ask website providers to test how many visitors their sites can handle before elections, when traffic increases.

The board should have a clear way for people to report website problems or security issues, referred to as a vulnerability disclosure policy (VDP). Make sure these reports go to the right people at the board (usually the technical person in charge of the website) so they can fix the problems.

ANNUAL CYBERSECURITY AWARENESS TRAINING

Board members and staff must take an approved security awareness training course every year and send proof of completion to the Secretary of State's office within 30 days of completion.

If the board doesn't have training available, the Secretary of State's office will provide it for free. Complete the training within two months of enrolling. If the board uses training from the Secretary of State's office, it doesn't need to send proof of completion.

PHYSICAL SECURITY ASSESSMENT AND TRAINING

Each board must complete a free DHS physical security assessment. Security assessments should be completed:

- Every three to five years.
- When a board moves to a new location (see also **Chapter 2, Board of Elections Location Move, Secretary of State/Board Coordination Checklist and Timeline**).
- When there is a significant remodel of the current board office.
- On notification from the Secretary of State.

This includes on-site visits and web-based surveys to find security gaps and suggest fixes. Boards should review the report, consider the recommendations, and conduct remediation to reduce any identified security vulnerabilities.

Boards must also train staff on physical security practices and policies. The rules for securing offices, voting equipment, and ballots are outlined earlier in **Section 3.03** of this chapter. Make sure board practices meet or exceed these standards.

CRIMINAL BACKGROUND CHECKS

All permanent board employees, vendors, and contractors who perform sensitive services must have a criminal background check. Sensitive services include access to personal or agency data, computer systems, or secure areas without supervision.

Vendors and contractors can either pay for their background check or attest to having completed one with no disqualifying crimes. Each board must have a policy for reviewing background checks and deciding who can be hired based on criminal history.

VENDOR CONTRACTS

Vendor partnerships should be closely evaluated and monitored for security risks. The board must work with its legal counsel to add cybersecurity terms to all new or renewed contracts for:

- Voter registration systems.
- Electronic pollbooks.
- Ballot-on-demand services.

- Voting machines.
- IT services.

These contracts must include a Security Supplement to ensure vendors follow the Ohio Secretary of State's official security directives.

The Security Supplement includes standard cybersecurity terms for data protection, network security, vulnerability management, access control, MFA, incident response, supply chain risk, and more. The federal government bans products from foreign vendors, and that ban applies to all contracts.

More details can be found in the Security Supplement. The Security Supplement covers:

- Data and network protection.
- Vulnerability management and application security.
- Controlling who has access.
- Password and authentication requirements.
- How to handle security incidents.
- Supply chain risks.
- Ban on foreign products.
- Software Bill of Materials.

Section 3.05 Security Event Reporting

This section defines "security events" and tells the board and its employees how to report them to the Secretary of State's office. The board must notify the Secretary's office immediately, even outside business hours, using the email in the *Security of Critical Infrastructure Security Directive*. Follow the instructions if email isn't available. Follow these instructions year-round, even if law enforcement is not involved.

Examples of Reportable Security Events include:

- Instances of any direct, indirect, or perceived threats of violence, harassment, or intimidation of election officials, staff, precinct election officials, or property used

by the boards of elections. If you believe a threat of violence is imminent, call 9-1-1.

- Someone without proper clearance is trying to get into board facilities, polling places, or offices.
- Phishing or hacking attempts on county voter registration systems or websites.
- Attempts to alter or destroy election-related systems (such as candidate qualifications, ballots, and voting equipment).
- Unauthorized access or inaccessibility of IT systems used for election management.
- Phishing or hacking of election officials' email or social media accounts.
- Hacks on political party or candidate IT systems.
- Disruptions or hacking attempts on absentee ballot infrastructure.
- Compromises of networks/systems affecting election-related infrastructure.
- Attempts to persuade officials to engage in illegal activity.
- Disruptions at polling or training locations that hinder voter participation.
- Disinformation efforts targeting government websites or voter participation.
- Unauthorized entry into vote-counting locations or election systems.
- Impacts to critical infrastructure (for example, the board's power, internet, transportation) affecting elections.

MARCS BACK UP EMERGENCY COMMUNICATIONS

The Secretary of State's office has provided each board of elections with a Multi-Agency Radio Communication System (MARCS radio) for backup communications and emergency preparedness. All boards must make sure they have enough staff trained to use the MARCS radio in case of an emergency. Be sure the radio is charged and turned on during all voting periods. Set it to the appropriate channel and store it securely when not in use.

Local law enforcement and boards will receive additional guidance before each statewide election to ensure proper usage if needed.

Chapter 3 Checklist: Security

PHYSICAL SECURITY

Office Security

- ☐ Create and adopt a comprehensive office security policy.
- ☐ Train all staff on the security policy.
- ☐ Implement visitor registration and supervision protocols.
- ☐ Restrict access to areas with voting equipment and systems.
- ☐ Establish a process for reporting security violations.

Voting Equipment Storage

- ☐ Secure voting equipment in a clean, climate-controlled area.
- ☐ Install a monitored security system for the storage area.
- ☐ Use a dual-control lock system that requires bipartisan access.
- ☐ Keep a visitor log for the storage area.
- ☐ Install smoke detection and fire suppression systems.
- ☐ Train staff on fire response.
- ☐ Keep the storage area clean.

Equipment Inventory

- ☐ Maintain complete inventory of all voting equipment with serial numbers.
- ☐ Keep purchase documentation for all equipment.
- ☐ Maintain Chain of Custody logs for at least two years.
- ☐ Track and log equipment usage, including date, location, and user.
- ☐ Document any damage or unauthorized handling.
- ☐ Keep complete repair history records.

- ☐ Regularly review the inventory list.

Ballot and Media Storage

- ☐ Store ballots and election media in a clean, secure, climate-controlled area.
- ☐ Give access to authorized people only.
- ☐ Use a dual-lock system for ballot storage.
- ☐ Store ballots according to printer directions.
- ☐ Mark and properly store all election media.
- ☐ Keep a detailed inventory of all ballots.
- ☐ Use Chain of Custody logs for ballot delivery.

SYSTEM SECURITY

Voting Systems

- ☐ Be sure that no voting machines connect to the internet.
- ☐ Only connect voting machines to air-gap networks when necessary.

Passwords and Access Control

- ☐ Set BIOS passwords on all vote tabulation servers.
- ☐ Implement split passwords with bipartisan control.
- ☐ Ensure passwords meet all complexity requirements.
- ☐ Change BIOS and central tabulating system passwords before every election.
- ☐ Set up automatic logout after 5 minutes of inactivity.

User Accounts

- ☐ Give each user a unique ID and password.
- ☐ Use complex password requirements.
- ☐ Use different passwords for different applications.
- ☐ Change passwords every 90 days.

- ☐ Set up multifactor authentication for all critical systems.
- ☐ Review user accounts quarterly.
- ☐ Keep administrative and regular accounts separate.
- ☐ Change service account passwords every year.

Logs and Monitoring

- ☐ Regularly check all access logs.
- ☐ Look for unusual access patterns or suspicious activity.
- ☐ Store logs on a separate system.
- ☐ Keep logs for 90 days.
- ☐ Do not turn off electronic logs.

IT SECURITY

Email and Website Security

- ☐ Use only .gov domains for websites and email.
- ☐ Never forward official emails to personal accounts.
- ☐ Use DMARC and DKIM email authentication.
- ☐ Set up Sender Policy Framework (SPF).
- ☐ Use MFA for all email accounts.
- ☐ Install TLS/SSL certificates on all web applications.
- ☐ Protect websites with a web application firewall.

Data Protection

- ☐ Back up voter registration server and data every day.
- ☐ Encrypt backups using FIPS 140-3 standards.
- ☐ Store backups in a secure, off-site location.
- ☐ Test backups annually to be sure they can restore data.

- ☐ Run weekly authenticated vulnerability scans.
- ☐ Fix critical issues within 15 days.
- ☐ Fix other vulnerabilities within 30 days.

SECURITY PROGRAMS AND TRAINING

CISA and MS-ISAC Resources

- ☐ Use Cyber Hygiene Vulnerability Scanning Service to find internet vulnerabilities.
- ☐ Use Web Application Scanning service for the board's website vulnerabilities.
- ☐ Request a Risk and Vulnerability Assessment every two years.
- ☐ Request Remote Penetration Testing every two years.
- ☐ Register new staff with the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC).
- ☐ Keep MS-ISAC contact information updated.

Response Planning

- ☐ Maintain an incident response plan.
- ☐ Conduct annual tabletop exercises (TTX).
- ☐ Submit updated plans to the Secretary of State's office.
- ☐ Have website providers perform load testing.
- ☐ Consider creating a vulnerability disclosure policy.

Training and Assessment

- ☐ Complete annual cybersecurity awareness training.
- ☐ Submit training completion certificates within 30 days.
- ☐ Complete DHS physical security assessment.
- ☐ Review and implement assessment recommendations.
- ☐ Train staff on physical security practices.

Vendor Management

- ☐ Conduct criminal background checks for permanent employees.
- ☐ Require background checks for vendors handling sensitive services.
- ☐ Include cybersecurity terms in all vendor contracts.
- ☐ Do not use products from foreign vendors banned by federal government.

EMERGENCY PREPAREDNESS

Incident Reporting

- ☐ Know what security events must be reported.
- ☐ Establish clear reporting procedures.
- ☐ Train staff to report incidents immediately.
- ☐ Know who to contact at the Secretary of State's office.

Emergency Communications

- ☐ Train staff on MARCS radio use.
- ☐ Keep MARCS radio charged during voting periods.
- ☐ Set MARCS radio to the appropriate channel.
- ☐ Store MARCS radio securely when not in use.