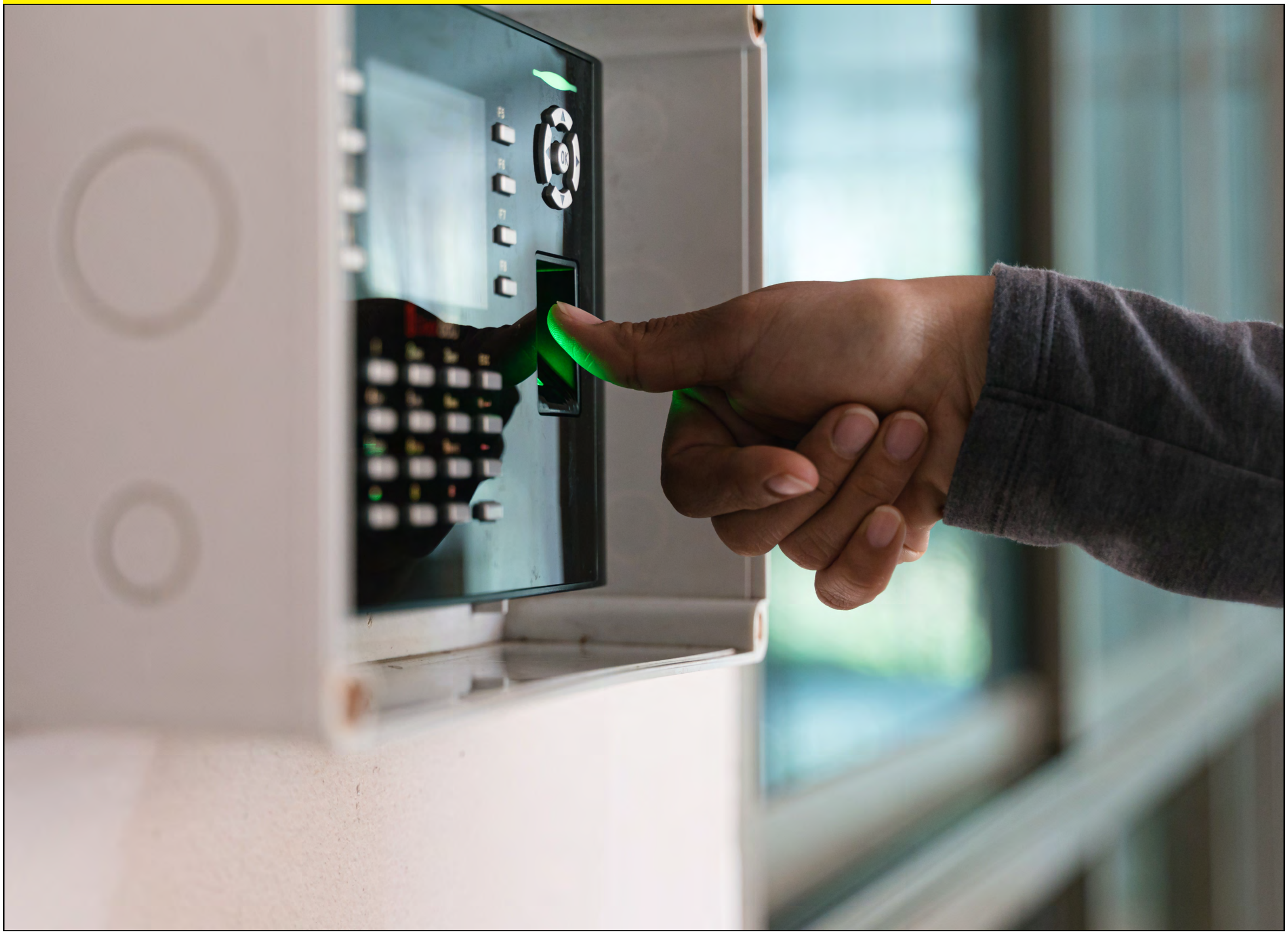


Chapter 2: Security

Chapter 2 Contents

27 Section 2.1: Physical Security

- ❑ Layers of Security
- ❑ Secure Storage Requirement

32 Section 2.2: Cybersecurity

- ❑ Core Security Principles
- ❑ Vendor Security
- ❑ Social Engineering

34 Section 2.3: Device Security

Section 2.1: Physical Security

RCW 29A.40, *RCW 29A.60*

Notes

Election security comprises both physical and cybersecurity components. Physical security serves as the base for robust cybersecurity measures. These combined efforts are aimed at safeguarding against unauthorized access to election sites and computerized systems.

Unfortunately, simply the appearance of unauthorized access will cast doubt on an election's integrity. Keep this in mind when making decisions about security.

Complex security methods, such as security cameras and electronic badge access, alone do not usually meet the requirements of secure storage, and they can provide a false sense of physical security.

Physical security refers to all policies, procedures, and actions taken to protect voting systems, equipment, required documentation, ballots, and related facilities from natural hazards, tampering, vandalism, and theft from both internal and external sources.

Secure storage includes the use of numbered seals and logs or other security measures that: "documents appropriate access and detects inappropriate access" of ballots, ballot images, and systems used to count and tabulate votes. (See WAC 434-256-045)

To ensure the most effective security measures, it's essential to have multiple layers of safeguards in place. Evaluate the security of your office and storage areas by considering the following six questions:

- ❑ How does the elections department restrict public access to sensitive areas?
- ❑ Are digital data, tabulation systems, storage areas, processing areas, and ballots in custody adequately secured?
- ❑ Do you utilize tamper-evident seals and maintain detailed logs to document access?
- ❑ Who is responsible for and how frequently are logs/documentation reviewed?
- ❑ Are staff members trained to identify signs of seal tampering?
- ❑ Have trainings been conducted on your security policies and procedures?

The answers to these questions are informed by RCW and WAC, along with individual county policies and procedures. By addressing these questions, you can better assess and enhance the security measures in your office and storage areas.

Notes

Layers of Security

- ❑ **Access Control** — Implementing access control measures such as gates, locks, and security personnel to restrict entry to authorized personnel only.
- ❑ **Surveillance Systems** — Installing security cameras, motion sensors, or other monitoring devices to detect and deter suspicious activity.
- ❑ **Security Guards** — Employing trained security personnel to patrol election sites and respond to security threats.
- ❑ **Alarms and Alerts** — Installing alarm systems or panic buttons to alert authorities in case of emergencies or security breaches.
- ❑ **Visitor Management** — Implementing procedures for easy identification of visitors, issuing visitor badges, and monitoring their activities while on site.
- ❑ **Emergency Preparedness** — Developing and implementing protocols for responding to emergencies such as natural disasters, protests, or security incidents.
- ❑ **Training and Awareness** — Providing training to election staff and volunteers on security procedures, emergency response protocols, and recognizing and reporting suspicious behavior.
- ❑ **Collaboration with Law Enforcement** — Establishing partnerships with local law enforcement agencies to coordinate security efforts, share intelligence, and respond to security threats effectively.

When implementing a new security measure, ask yourself: What happens when the battery dies, or the power goes out? Can your system maintain secure storage when the unexpected happens?

Secure Storage Requirement

WAC 434-256-045

While greater physical security can be implemented in varying degrees based on available resources, seals and logs are the simplest and most cost-effective way to assure proper storage of ballots and voting systems. There are three required elements for effective use: seals, logs, and policies and procedures.

- ❑ Seals must be:
  - ■ Uniquely numbered
  - ■ Tamper evident
  - ■ Logged when applied or removed
- ❑ Logs must included:
  - ■ Dates of application and removal
  - ■ Seal number
  - ■ Identifying information of persons attaching or removing seal
  - ■ The reason a seal was removed after tabulation
- ❑ Policies and Procedures
  - ■ Written procedures should stipulate how seals are to be installed, tested upon installation, and how to identify tampering before removal. Training should include identifying tampering on each type of seal that's used

Notes

What Materials Must Be Secured?

Ballots

The term "ballots" is not restricted to printed ballots. Ballots may mean:

- ❑ Any voted ballot
- ❑ Scanned ballot images
- ❑ Any electronic record of the choices of an individual voter, such as a cast vote record
- ❑ All emails containing voted ballots
- ❑ Data such as mobile ballot boxes on removable storage devices
- ❑ Programmed tabulators

Voted ballots and ballot images must be in secure storage except when two staff are present during:

- ❑ Initial and final processing
- ❑ Duplication
- ❑ Inspection by the canvassing Board

Whenever ballots are not in secure storage, two elections officials must be present for all steps of ballot processing.

Following tabulation, seal ballots in containers that identify the primary or election. Only open containers sealed after tabulation for the following reasons:

- ❑ Canvass of ballots prior to certification.
- ❑ Recounts conducted per Canvassing Board directive.
- ❑ Manual audit per RCW 29A.60.170(3).
- ❑ Order of the superior court.
- ❑ Consolidation into one container for storage purposes.

Notes

Be sure to document access. This can be included on the seal log. When the Canvassing Board opens a ballot container, include a full record of the additional tabulation or examination of ballots in the Canvassing Board documents.

Unsealing ballots during an election must be open to public observation.

Voting Devices

Preparation of a voting device for a primary or election must include:

- ❑ Complete test logs which indicate precincts tested.
- ❑ Sealing the device with a uniquely numbered seal to verify the programming has not been altered.

Ballot Deposit Sites

During an election, keep ballot deposit boxes locked and sealed at all times. Document each time a box is sealed and/or a seal is broken. Two people, either employees or appointees of the County Auditor, must empty ballot deposit boxes together (see WAC 434-250-100).

At exactly 8:00 p.m. on Election Day, all ballot boxes must either be:

- ❑ Emptied, or
- ❑ Secured with a numbered seal to prevent deposit of ballots after 8:00 p.m.

Transport ballots to the counting/processing center by either:

- ❑ At least two authorized people together, or
- ❑ One person with the ballots in containers secured by two authorized people with seals and logs.

Ballot Tabulation Programming

Secure storage is required of all tabulation equipment including:

- ❑ Scanners
- ❑ Printers
- ❑ AVUs
- ❑ Data and Databases

Your practices should include:

- ❑ Never allowing a vendor or employee uncontrolled access to equipment.
- ❑ Limiting access to authorized personnel only and documenting all access.
- ❑ Showcasing your procedures when the public observes logic and accuracy tests, ballot processing, recounts, and other election activities.
- ❑ Including these in your procedures: use of seals/logs, employee monitored entrances/exits, a sign-in/sign-out log, and visitor name tags, badges, colored lanyards, etc.

Best Practices for Physical Security

Seals

Seals are only as good as their use protocol.

- □ Use written procedures that stipulate how seals are to be installed, tested upon installation, and how to identify tampering before removal.
- □ Training should include identifying tampering on each type of seal that's used.
- □ Logging an entire inventory of seals and seal numbers to be used in each election.

Seal Types

Select a type of seal that is compatible with the application.

- □ Sticker seals should generally be sold as no residue or low residue stickers. Leftover residue can impede tamper evidence if not cleaned before the new seal is applied.
- □ A low strength plastic pull tight seal should be reserved for indoor controlled environments. Plastic seals are susceptible to heat, cold and prolonged outdoor exposure.
- □ Seals utilizing aluminum and steel construction are best when applied to outdoor ballot drop boxes. These seals are designed to resist exposure to the elements and add an increased barrier to entry. Tampering with these seals requires a much higher threshold of effort.
- □ It's preferable, but not necessary, that the vendor for seals will sell only to governmental agencies and not the public.

Locks

When possible, locks should:

- □ Be made of durable material. Outdoor locks should be weather-resistant.
- □ Employ proper key control. All keys should be tracked and kept to a minimum.

By design, locks do not detect or document access. Locks alone do not meet the requirements of secure storage.

For more information about election security best practices, contact the Certification & Training or Information Security and Response programs at the Office of the Secretary of State. See also the Election Security page on the U.S. Election Assistance Commission website.

Notes

Notes

Section 2.2: Cybersecurity

Cybersecurity is the practice of reducing the risk of cyberattacks. Computers, mobile phones, servers, electronic systems, and networks are at risk for attack. Systems critical for election security include:

- ❑ IT infrastructure and systems used to manage elections.
- ❑ Voter registration databases (VoteWA) and associated IT systems.
- ❑ Voting systems (tabulation equipment).
- ❑ Storage facilities for election and voting systems.
- ❑ Vendor Security.

Cybersecurity is important for everyone because digital products play a central role in our daily lives.

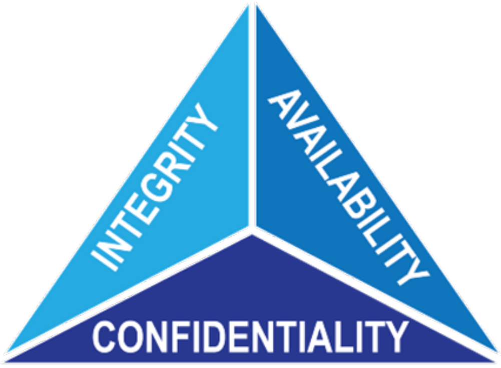
Core Security Principles

One of the basic principles of providing a secure system is to manage risk and protect sensitive information. The goal is to keep data private, unchanged, and available. This concept is known as the Confidentiality, Integrity, and Availability (C.I.A.) Triad. Each attempted cyberattack seeks to violate one or more of the triangle's attributes.

Confidentiality — Private information is kept private by preventing unauthorized access.

Integrity — Protecting data from unauthorized changes.

Availability — Ensuring data and services are available only to authorized users when needed.



Vendor Security

Attackers may attempt to bypass security in a state or county government facility by targeting a vendor first. For this reason, there is a need to address cyberthreats associated with vendors and other third-parties that have trusted permissions.

Conduct thorough assessments and use due diligence before engaging with vendors to ensure they have appropriate security measures in place. This includes reviewing their security policies, procedures, certifications, and past security incidents.

For assistance or questions regarding vendor security please contact cybersecurity@sos.wa.gov and for policy questions ctsupport@sos.wa.gov.

Social Engineering

Social engineering is when cybercriminals trick individuals into breaking normal security procedures and best practices to gain access into systems, networks, or physical locations.

Social engineering is accomplished in many ways (online, telephone, shoulder surfing, simple persuasion). Social engineering is one of the hardest attacks to protect against, and it is the most prevalent.

Phishing

Phishing is a social engineering tactic used to persuade individuals to provide sensitive information and/or take action through seemingly trustworthy communications. Phishing emails may attempt to appeal to a recipient’s fear, duty, obligation, or curiosity.

Distributed Denial of Service

Distributed denial of service (DDoS) uses multiple compromised computers to overwhelm a network causing network traffic to stop, much like a traffic jam causing a gridlock on a highway. Computers are often infected through phishing attacks that trick the user into downloading malicious files.

Ransomware

Ransomware is an advanced form of malware that can encrypt all data saved on a computer. To unlock the data, a payment is demanded. In elections, cybercriminals seek not only monetary gain but to cast doubt on the democratic process and integrity of elections.

Ransomware uses social engineering tricks to exploit potential victims. Spam emails are a typical method to send out attacks to potential victims. They are designed to look like they are from a legitimate source. Once a user clicks a malicious link or attachment, the ransomware is downloaded and installed on the computer. It then begins to encrypt data so only the hacker can read it.

Notes

Notes

Section 2.3: Device Security

External Storage Devices

Whether you are building your ballot, uploading election results, or importing information from a sorter that isn't connected to a network, you will eventually need to securely transfer data with an external memory device. Whenever you are connecting a device to any computer, there is the risk of compromising that computer. It is, therefore, critically important that only secure devices are connected to your systems.

A new, securely wiped and tamper-evident sealed USB should be used to import or export data to or from the air-gapped tabulation system networks.

Read-only USB Drives

Reusable read-only USB drives are an alternative to sealed one-time-use USB drives. The read-only feature, activated by a clearly-visible switch on the outside of the device, gives users control over whether or not their tabulator or computer can exclusively pull (read) data from the device or if they can also add (write) new data to it.

To maintain proper security, you must first wipe (format) the USB drive just before inserting it into your air-gapped tabulator. This further ensures that no data will be introduced to your tabulator.

The Office of the Secretary of State has a program to supply each county elections office with suitable devices and formatting equipment.

Mobile Devices

Have you addressed your mobile device security? What people are targeting on a desktop can now be accessed on mobile devices. "Mobile Device Security" refers to the measures taken to protect sensitive data stored on portable devices, such as smart phones and laptops. It prevents unauthorized users from using mobile devices to access your network.

ⓘ *For support and questions regarding security please contact cybersecurity@sos.wa.gov*