Elections Security

A critical part of election administration is security. Security comprises physical and cybersecurity. Physical security lays the foundation for cyber security. These protect against unauthorized access to elections physical locations and computerized systems.

Chapter 2, Section 1

Physical Security

RCW 29A.40, 29A.60

Physical security expands beyond the perimeter of the building and includes laptops and mobile devices.

Security Layers

Physical Security: refers to 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 employs physical security and the use of numbered seals and logs or other security measures that detect any inappropriate access to secured materials.

Multiple layers of safeguards create the most effective security. Evaluate the physical security and secure storage of your office by answering these five questions:

- How does the elections department restrict public access?
    - Digital Data, Tabulation Systems, Storage Areas, Processing Areas, Ballots in Custody?
- Do you have tamper-evident seals and logs always documenting who accessed ballots?
- Are your seals and logs appropriate for the application/environment?
- Who reviews the access log/documentation and how often?
- Have you conducted trainings on your security policies and procedures?

Physical Security
WAC 434-256-045

Physical Security Examples

- Electronic surveillance such as video
- Electronic keycard systems with automatic logs.
- Tabulator sign-in logs (not a seal)

NOTES:____

____

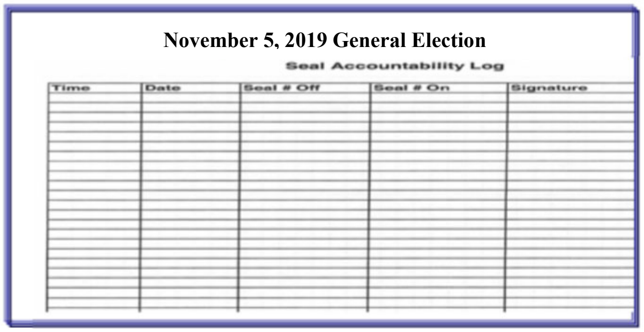
____

- Other methods that detect and document access to secured materials.

Secure Storage of Ballot Images

Seals and logs must be used for the storage handling of ballots and tabulation systems.

- Seals
  - Uniquely numbered
  - Seals retained and logged when broken
  - 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.
- Logs
  - Chronological dates of application and removal
  - Seal number
  - Identifying information of persons attaching or removing seal
  - Documentation as to why a seal was removed after tabulation



November 5, 2019 General Election

Seal Accountability Log

Time	Date	Seal # Off	Seal # On	Signature

What materials must be secured?

Ballots

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

- Any voted ballot.
- Scanned ballot images.
- Emails, including deleted emails, containing voted ballots.
- Tally documents.
- Data, such as mobile ballot boxes (MBBs, Zip Drives, USB drives, V-drives).
- Programmed tabulators.

Voted ballots and ballot images must be in secure storage except during:

- Initial and final processing.
- Duplication.
- Inspection by the Canvassing Board.

NOTES:____

____

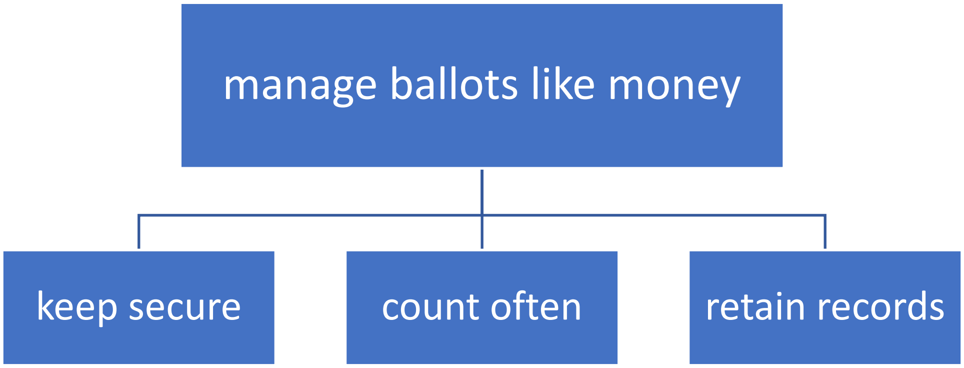
____

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.

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.

Notify political parties and request observers whenever unsealing ballots.



Voting Devices

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

- Complete test logs which indicate precincts tested.
- Sealing the device with a uniquely numbered seal.

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.

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.

NOTES:____

____

____

Transport ballots to the counting/processing center by either:

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

Ballot Tabulation Programming

Security measures apply to ballot tabulators. Secure tabulation equipment (including AVUs), databases, and data. Limit access to authorized personnel only and document all access.

ⓘ *Optical scan systems must follow an approved security plan when scanning before Election Day.*

Physical Security Best Practices

Seals

Seals are only as good as their use protocol. 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.

- Select a type of seal that is compatible with the application:
    - Sticker seals should generally be no residue or low residue stickers. Left over residue can impede tamper evidence if not cleaned before the new seal is applied. Sticker seals should be tested to resist common chemicals.
    - 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. Being easily broken, these seals can be used to support a narrative of unsecure elections due to ease of removal.
    - A steel cable seal should be used when the container to be sealed is left outdoors or unattended. 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.
- When possible, employ seals and locks that meet or exceed current ISO (the International Organization for Standardization) 17712 standards. When applicable, manufacturers should be willing to provide certificates of compliance and test data to support their claims.
- It's preferable, but not necessary, that the vendor for seals will sell only to governmental agencies and not the public.
- If video cameras are used, schedule regular checks to make sure they are operational.
- Implement two-person integrity policies when setting up a voting system. Never allow a vendor or employee uncontrolled access to equipment.
- Only authorized election staff should be allowed in the scanning and tabulation areas.

NOTES:____

____

____

- Unless actively processing, ballots are always stored in a secured area with restricted access.
- Provide visitors with clear procedures when observing logic and accuracy tests, ballot processing, recounts, and other election activities. These procedures should include the use of employee monitored entrances and exits, a sign-in/sign-out log, and physical identifiers such as visitor name tags, badges, colored lanyards, etc.

Locks

- Door locks should be graded by the American National Standards Institute (ANSI) grade, with Grade 1 the most secure and Grade 3 the least. Grade 1 should be specified.
- When purchasing padlocks, utilize locks with CEN (Central European Norm) 4 or higher rating for high security.
- Practice adequate key control. The number of keys to access a secured area or to empty drop boxes should be kept to a minimum and all keys should be tracked. Audit keys and key holders regularly to assure all keys are accounted for. Similar protocols should be employed with badges.
- If video cameras are used, schedule regular checks to make sure they are operational and that there is sufficient video storage for the purpose of the review of footage.
- Implement two-person integrity policies when setting up a voting system. Never allow a vendor or employee uncontrolled access to equipment.
- Only authorized election staff should be allowed in the scanning and tabulation areas. Video cameras provide an extra layer of security.
- Review chain-of-custody procedures, the use of tamper-evident seals and inventory control/asset management processes.

- Unless actively processing, ballots are always stored in a secured area with restricted access.
- Provide visitors with clear procedures when observing logic and accuracy tests, ballot processing, recounts, and other election activities. These procedures should include the use of employee monitored entrances and exits, a sign-in/sign-out log, and physical identifiers such as visitor name tags, badges, colored lanyards, etc.

NOTES:____

____

____

Chapter 2, Section 2

Cybersecurity

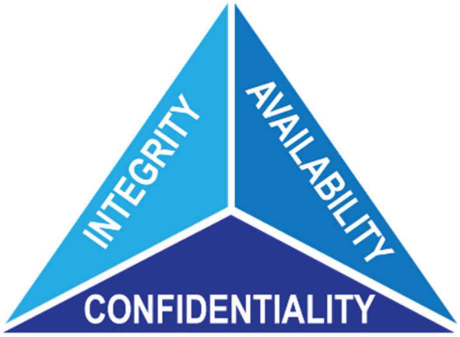
Cybersecurity is the practice of reducing the risk of cyber-attacks. Computers, mobile phones, servers, electronic systems, and networks are at risk for attack. Systems critical for election security include:

- IT infrastructure and systems used to manage elections.
- Voter registration databases 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 cyber-attack seeks to violate one or more of the triangles attributes.



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

- Make sure that everyone and everything that accesses data verifies identity in some way. Methods include a password or PIN, smart card, or fingerprint.
- Permissions allow access to data only to authorized users and no one else.
- Encryption scrambles and conceals the data in a format where the only way you can see the data is if you have a key.

NOTES:____

____

____

Integrity – Protecting data from unauthorized changes.

- Use specialized software that monitors for suspicious activity and notifies someone if there are unauthorized changes to data.
- Keep systems current and upgrade when necessary.

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

- Tune network devices to monitor for Distributed Denial of Service attack.
- Keep systems current.
- Back up and store data in an offsite location.

ℹ *Just the appearance that system access was gained will cast doubt on an election's integrity.*

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) and is one of the hardest attacks to protect against and is the most prevalent. It is dangerous because the malicious actor does not need any technical skills. Social engineering is effective because people are the weakest link.

There are several methods to launch a social engineering attack.

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.

How to Identify a Potential Phishing Attack

Ways to recognize phishing emails include:

- Be aware of someone that wants too much information.
- Urgent action warning of major consequences.
- Spelling and grammar errors.
- Link to a website.
- Request for personal information.
- Pop-up ads.

NOTES:____

____

____

Signs an attack could be in progress include:

- Computer is unresponsive.
- Drives or files are unavailable.
- Data files are transferring at a higher than normal rate.

How to Avoid a Phishing Attack and How to Respond

There may not be any indication of an attack at all. You can reduce the likelihood of an attack by:

- Not opening any attachments or following links included in emails unless you are sure it is safe. Consider contacting the sender via an out-of-band communication. For example, consider contacting the sender of a suspicious email by calling a known phone number.

If you think you are the victim of a phishing attack, take action immediately:

- Follow county procedures for reporting a potential phishing attack.
- Unplug the network cable.
- DO NOT turn off the computer.

Distributed Denial of Service (DDoS)

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. In order 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 it is downloaded and installed on the computer. It then begins to encrypt data so only the hacker can reit.

NOTES:____

____

____

Chapter 2, Section 3

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 cyber threats associated with vendors and other third-parties that have trusted permissions. Evaluating a vendor's security policies is a way to assure data security on their end and it helps to define what actions to take if a breach occurs.

Questions to ask vendors include:

- How do the vendors and their employees understand and practice security?
- How and where do they secure data?
- What is the vendor's Disaster Recovery Plan?

An active and dedicated information security team can make a huge difference when things "hit the fan."

NOTES:____

____

____

Chapter 2, Section 4

Mobile Devices

Mobile devices have a huge impact on our day-to-day lives and the way we communicate with the world. We shop, communicate with friends, bank, play games, watch movies, and work. It is common for employees to use their smartphones to check emails, access shared drives, or to share information with others.

With smartphones used as an all-in-one computing device for work and personal use, they make an attractive target for cybercriminals. What people are targeting on a desktop, they are now targeting more 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.

Mobile Device Best Practices

Best practices for mobile devices include:

- Avoid public Wi-Fi. Often when connecting to Wi-Fi networks, the assumption is they are safe for use. However, hackers can easily access the network and steal data.
- Use strong passwords. Just as within the network, mobile devices should also require strong passwords.
- Use different passwords for all accounts, including email and social media.
- Do not download any unauthorized applications. Often the user believes the site is reputable, but instead it is a bogus app designed to look like it is genuine.
- Include mobile device security in training programs.

NOTES:____

____

____