

CHAPTER 6 – ELECTIONS SECURITY
TABLE OF CONTENTS

6.1 Physical security..... 2
 Which materials must be secured?3
 Physical security best practices.....5
 6.2 Cybersecurity 5
 Information security5
 Cyber attacks - Social engineering7
 6.3 Vendor security..... 9
 6.4 Mobile devices 10

NOTES: _____

ELECTIONS SECURITY

A critical part of election administration is security. Security comprises physical and cybersecurity. Both protect against unauthorized access to elections physical locations and computerized systems.

6.1 PHYSICAL SECURITY

RCW 29A.40 & 29A.60

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

DEFINITION

WAC 434-250 & 261

Secure storage employs the use of numbered seals and logs or other security measures that detect any inappropriate access to secured materials. When access is detected, security methods detect which election materials were accessed.

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

1. How does the elections department restrict public access to critical areas?
2. How do you restrict access to records, computers containing data, tabulation, processing and storage areas?
3. Do you log/document who accesses ballots? Every time?
4. Who reviews the access log/documentation and how often?
5. Can your security measures identify which materials were accessed and by whom?

SECURITY LAYERS

Security layers may include:

- Seals.
 - Uniquely numbered.
 - Destroyed when accessing ballots/secured areas.



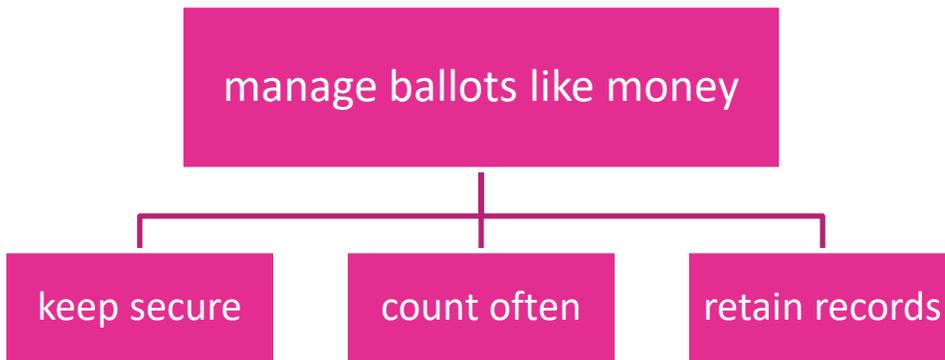
NOTES: _____

- 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.

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.

NOTES: _____

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.

- ① *Optical scan systems must follow an approved security plan when scanning before Election Day.*

PHYSICAL SECURITY BEST PRACTICES

- Protect equipment with monitored security and fire alarm security.
- 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. 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

6.2 CYBERSECURITY

Cybersecurity is the protection of internet-connected systems. This includes protecting hardware, systems, and data from cyberattacks.

INFORMATION SECURITY

A subset of cybersecurity is Information Security. Information Security refers to the steps administrators and staff must take to ensure the confidentiality, integrity, and availability of elections; including but not limited to:

- Voter registration databases and associated IT systems.
- IT infrastructure and systems used to manage elections.

NOTES: _____

- Voting systems (tabulation equipment).
- Storage facilities for election and voting systems.
- Vendor Security.



CIA Triangle

Confidentiality – Data is only accessed by those who have authorization on a need to know basis. Sensitive information is protected.

Integrity – Data has not been modified. Information is trustworthy and accurate.

Availability – Information and resources are available when requested.

Each attempted cyber-attack seeks to violate one or more of the triangle's attributes.

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

The Defending Digital Democracy Project at the Harvard Kennedy School outlines five key points every election staffer needs to know and observe about cybersecurity:

1. Everyone is a security official. Everyone is responsible for being vigilant and reporting irregularities.
2. Use two-factor authentication to protect your access credentials for elections systems, email, social media, and data storage.
3. Create long, strong passwords.
4. Keep credentials secure and never share them with anyone, regardless of who they are.
5. Use best practices for cyber hygiene, including installing patches, software updates and up-to-date antivirus software.

NOTES: _____

Employees often do not know they are compromising security. The security landscape is constantly changing making ongoing security training essential.

CYBER ATTACKS - SOCIAL ENGINEERING

Social engineering is a key concern and a broad term for malicious activities that involve tricking people into breaking normal security procedures and best practices in order to gain access into systems, networks or physical locations.

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 recipients fear, duty, obligation, or curiosity.

HOW TO IDENTIFY A POTENTIAL PHISHING ATTACK

Ways to recognize phishing emails include:

- Urgent action warning of major consequences.
- Spelling and grammar errors.
- Link to a website.
- Request for personal information.
- Pop-Up ads.

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.

NOTES: _____

HOW TO AVOID A PHISHING ATTACK AND HOW TO RESPOND

There may not be any indication at all of an attack. 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.

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.

The YouTube video, “Phishing Explained”, produced by Ecourse Review, (<https://www.youtube.com/watch?v=PTE2oqMcfSw&feature=youtu.be>) addresses how to identify a potential email scam or phishing attack.

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 (usually in Bit Coin) is demanded. In elections, cybercriminals seek not only monetary gain but seek to cast doubt on the democratic process and the 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 design 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 read it.

NOTES: _____

6.3 VENDOR SECURITY

As many security breaches have occurred by targeting vendors first, there is a need to address cyber threats associated with them. 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: _____

6.4 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 not uncommon 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. In reality, 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: _____

