CHAPTER 6 – ELECTIONS SECURITY
TABLE OF CONTENTS

NOTES: _____

_____

_____

ELECTIONS SECURITY

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

6.1 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 which 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.
- Voting systems.
- 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 triangles attributes.

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

NOTES: _____

_____

_____

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.

Employees often don't 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** is a form of attack that appears to be from a trusted source. The attacker uses an email or other electronic communication to distribute a malicious link or attachment.

  During the 2016 Presidential Election, Arizona Elections was hit with a phishing attack. Arizona elections had its voter registration system breached when an employee fell victim to a phishing scheme and downloaded a virus that leaked credentials online. Access to their voter registration systems was gained.

- **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.

  During the 2018 mid-term elections, Knox County, TN was hit with a DDoS attack. Election night results were delayed.

- **Ransomware** is an advanced form of malicious malware that can encrypt all data saved on a computer. In order to unlock the data, a payment (usually in Bit Coin) is

NOTES: _____

_____

_____

demanded. In elections, cybercriminals 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 encode the data it a way that only the hacker can read it (encryption).

Targeted ransomware attacks on US government entities are on the rise regardless of their size. The largest major city to be hit was Baltimore which included the board of elections. Smaller jurisdictions have also seen an increase in ransomware. One of which was Madison County, Idaho with a population of approximately 40,000.

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.

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. If in doubt contact the sender.

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

- Unplug the network cable.

NOTES: _____

_____

_____

- DO NOT turn off the computer.
- Follow county procedure for reporting a potential cyber attack.

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.

6.2 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 lap tops and mobile devices.

DEFINITION WAC 434-250 & 261

Secure storage employs the use of numbered seals and logs or other security measures which 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 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, and 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 accessed and by whom?

SECURITY LAYERS

Security layers may include:

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

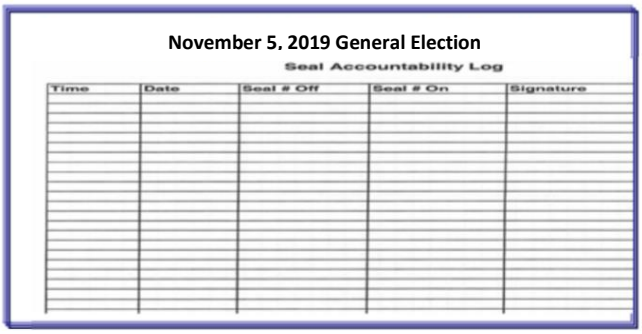
NOTES: _____

_____

_____

- 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

- Electronic surveillance
- Electronic keycard systems with automatic logs
- Other methods that detect and document access to secured materials



November 5, 2019 General Election

Seal Accountability Log

Time	Date	Seal # Off	Seal # On	Signature

WHICH 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

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

NOTES: _____

_____

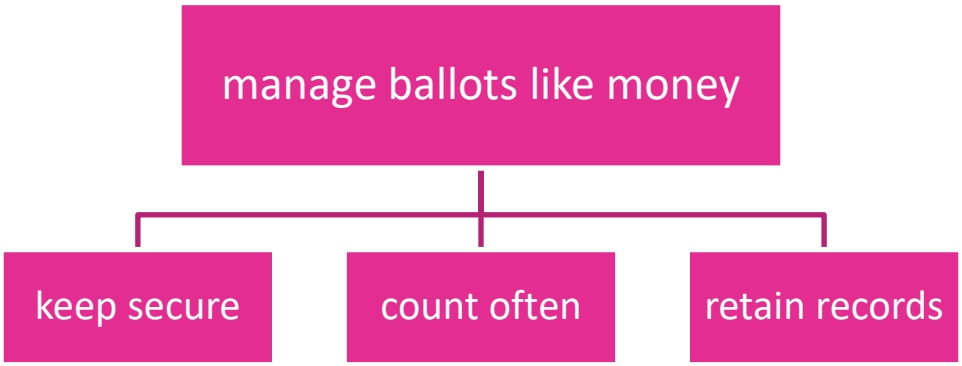
_____

- 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.

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:

- Making a record of the ballot format installed in each device and the precinct the voting device will serve.
- Sealing the device with a uniquely numbered seal.

Record the seal number on a log. From the time of receipt until opening, secure all returned ballot envelopes with voted ballots.

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 programming. 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

- Protect equipment with monitored security and fire alarm security. If video cameras are used, schedule regular tests to assure they are operational.
- 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, recounts and other election activities. These should include employee monitored entrances and exits, a sign-in/sign-out log.

NOTES: _____

_____

_____

6.3 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's 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 a long password for all accounts, including email and social media. A string of words that can be easily remembered but difficult to guess is one recommendation.

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.

For example, an employee downloads an app thinking it is from a trusted source. However, it is an app that is full of malware. The employee inputs usernames and passwords and from there the hacker can access the device, the company network and important data.

Include mobile device security in training programs.

NOTES: _____

_____

_____

6.4 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?
- Where do they store and how 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: _____

_____

_____