ELECTIONS SECURITY BEST PRACTICES

STRONG PASSWORDS

- Change them often (a good practice is changing them quarterly)
- The longer the better. Avoid short and easy phrases
- Passwords should include lowercase, uppercase, symbols and numbers if possible
- Don't share passwords
    - Do not write them down (no post-it notes)

BE AWARE OF SPEAR-PHISHING

Avoid websites with browser alerts AND emails that contain links or attachments.
Three indicators of spear-phishing are:

1. Grammar that is incorrect or does not make sense
2. Short messages that ask you to click a link or download an attachment
3. The address itself is off; an example of this could be:

   support@utah.gov could read as utah@support.com or supportt@ut.gov

RESTRICT REMOVABLE MEDIA

If your county uses USBs or any other type of removable media in regards to the election process:

- Limit their use
- Limit access to them
- Lock them up when not in use

NO PERSONAL USE

- There should not be any documents saved, systems used, or any other form of work in the elections process done on a system that is not properly connected or a device that can be easily interfered with.
- Do not create personal accounts using work emails

TIMELY MAINTENANCE / PATCHES

If your system needs to be maintained or patched, ensure that it is done ahead of the election, and in a timely fashion. It should never be done close to the election.

SUPPLY CHAIN HACKS

Be aware of where the updates are coming from. If the usual file is Mongoose.xxx and one pops up for Mongose.xxx (missing the second "o" in Mongo*o*se), it should not be clicked on, downloaded, or used.

MINIMUM ACCESS

- Only cleared employees should have access to VISTA, be sure to delete rights to those who have left.
- Monitor user activity, and have employees sign agreement understanding that they are being monitored.
- Restrict rights of users, not everyone should have delete rights just because they need to be able to view the system.
- Lock the computer anytime you walk away

SECURE NETWORK CONNECTIONS

If one webpage or system is somehow connected to the outside, be it through other systems or the internet, it leaves a window in for hackers. Ensure that any election related system is not vulnerable.

KEEP VISTA ACCURATE

VISTA is backed up nightly, and ESS can track anomalies. If anomalies are detected have a plan in place as to how they are to be investigated and corrected.

INCIDENT RESPONSE PLAN

Every county should have a plan in which they have clear instructions for themselves on what to do if anything were to go wrong.

- There are anomalies in audits
- If a system were to shut down
- Voters needing to cast provisional ballots.

*Voter confidence is imperative. Ensuring that all the precautions and stops are being taken boosts voter confidence.

SOCIAL ENGINEERING

Attackers often impersonate credible accounts to disseminate inaccurate information. Be aware and on the look out for this type of social media.

It's important to be aware of who follows you on social media, whether it is the county's page or yours personally. Individuals that follow you, personally or otherwise, may be using social media to develop relationships and gain information

ON ELECTION DAY

1. Cover spaces where removable devices may be inserted (electrical/duct tape will work)
2. Print out a paper copy of poll book (in case digital poll books are compromised)
3. Always allow individuals to vote provisionally
5. Be sure to have a communication plan ready and in place with:
    - Employees
    - The Authorities
    - The State (and subsequent system administrators)