2018 Election Cybersecurity Planning Snapshot
Polk County

ACTIVITIES / SAFEGUARDS

Iowa Election Process

Voters Registered
- Voter registration database is protected by firewall and security updates.
- Database is secured through Access Control Listing (whitelisting) and two-factor authentication.
- Users receive security training and follow strict security protocols.
- Database backups and contingency plans in place.

Voters Checked In
- Voter presents ID and is matched to voter database.
- Ballot security: Precinct officials safeguard ballots at all times.
- It is illegal to take a ballot from the polling place, curbside voting, or from a drop box.

Ballots Cast
- Iowa’s elections are paper ballot-based with electronic tabulation; the paper ballot is the official record.
- Ballots are securely stored with extensive chain-of-custody records.
- Electronic and physical security measures ensure voting system integrity on Election Day.

Results Released
- Results are unofficial until the canvass of votes.
- Canvass compares printed report from precincts to number of voters at polls and ballots cast before certifying results as official.

Post-Election Risk Safeguards

Voting, Tallying, & Reporting Systems
- County-specific security protocols in formalized policy.
- Vigorous logic and accuracy testing before election.
- Voting systems are not connected to the internet.
- Votes are counted in a secure location.

Election Results canvassed
- Results are unofficial until the canvass of votes.
- Canvass compares printed report from precincts to number of voters at polls and ballots cast before certifying results as official.

Post-Election Risk Safeguards

Election Results Canvased
- Results are unofficial until the canvass of votes.
- Canvass compares printed report from precincts to number of voters at polls and ballots cast before certifying results as official.

Election Day Security Guidelines

From Office of the Secretary of State Pursuant to Iowa Code 45.52B
- Ballot security: Precinct officials must safeguard ballots at all times. It is illegal to take a ballot from the polling place, curbside voting is the only exception. PEDs should report any person removing a ballot from polling place to the county auditor immediately.
- Equipment security: Precinct officials must safeguard voting equipment and all accessories at all times. Do not allow unauthorized persons access to this equipment. Only persons with written authorization from the county auditor may attempt to repair or replace malfunctioning machines. Call the County Auditor’s Office immediately if any of the security seals are broken.

Voting, Tallying, & Reporting Systems
- County-specific security protocols in formalized policy.
- Vigorous logic and accuracy testing before election.
- Voting systems are not connected to the internet.

Election Results released
- Results are unofficial until the canvass of votes.
- Canvass compares printed report from precincts to number of voters at polls and ballots cast before certifying results as official.

Election Day Security Guidelines

From Office of the Secretary of State Pursuant to Iowa Code 45.52B
- Ballot security: Precinct officials must safeguard ballots at all times. It is illegal to take a ballot from the polling place, curbside voting is the only exception. PEDs should report any person removing a ballot from polling place to the county auditor immediately.
- Equipment security: Precinct officials must safeguard voting equipment and all accessories at all times. Do not allow unauthorized persons access to this equipment. Only persons with written authorization from the county auditor may attempt to repair or replace malfunctioning machines. Call the County Auditor’s Office immediately if any of the security seals are broken.

THREAT MITIGATION

Specific Threats / Mitigation

Social Engineering: refers to tactics to steal personal information.
- Do not click on suspicious links in emails or texts.
- Be cautious when providing personal information online.

Information Operations: refers to tactics to manipulate public perception.
- Do not share sensitive information on social media.
- Be cautious when sharing information.

Information Operations: refers to tactics to manipulate public perception.
- Do not share sensitive information on social media.
- Be cautious when sharing information.

Vigorous logic and accuracy testing before election.
- Voting systems are not connected to the internet.

Hacking refers to attacks that exploit vulnerabilities in a system to disrupt or gain unauthorized access.
- Maintain up-to-date software and firmware.
- Use strong, unique passwords.

2018 ELECTION INITIATIVES

Polk County Overview

Precincts – 177
Active Voters – 281,315 (as of June 2018)
Optical Voting System / Model – Unisyn OVO v. 1.33M
Accessible System / Model – Unisyn OVI VC
Website – www.polkcounty.iowa.gov/auditor/election

2018 Activities & Timeline Checklist

Initiative 1: Cybersecurity workshop with auditors and IT staff from across the State
(Target Completion: June 22)

Initiative 2: Register for the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) at https://eiisc.org/ei-isac-registration
(Target Completion: July 15)

Initiative 3: Develop County Incident Response Plan including Reporting Matrix
(Target Completion: August 1)

Initiative 4: Schedule Cyber Hygiene Scanning. Contact ncciccustomerservice@hq.dhs.gov and reference “Iowa Cyber Hygiene Initiative” to obtain this service free through DHS
(Target Completion: September 1)

Initiative 5: Complete “Securing the Human Training.” Contact Voters.support@sos.iowa.gov to schedule
(Target Completion: September 1)

Initiative 6: Register for services provided by the Iowa Office of the Chief Information Officer
(Target Completion: September 1)

For Additional Information or Questions
Iowa Secretary of State’s Office: Ken Krueger, Deputy Commissioner of Elections, ken.krueger@iowa.gov
Geoffrey Jenista, Region VII Cybersecurity Advisor, Geoffrey.Jenista@hq.dhs.gov
PM Kirk, Region VII Director for Infrastructure Protection, pmkirk72@hq.dhs.gov

Recognizing and Reporting an Incident

Definition of an Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices (NIST Pub. 800-61)

If you suspect a Cybersecurity Incident has occurred, contact—
- Iowa Office of the Chief Information Officer - Information Security Division, (515) 281-5603 or https://iowa.gov/iowasecurity-security-security
- National Cybersecurity and Communications Integration Center (NCCIC), (888) 282-0870 or NCCIC@dhs.gov
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) Security Operation Center, (866) 767-4722 or sec@iowasecurity

In the event of a Data Breach, notify—
- Iowa Office of the Attorney General - Consumer Protection Division, consumer@iowa.gov
- Iowa Office of the Chief Information Officer - Information Security Division, informationsecurity@iowa.gov

For Additional Information or Questions
Iowa Secretary of State’s Office: Ken Krueger, Deputy Commissioner of Elections, ken.krueger@iowa.gov
Geoffrey Jenista, Region VII Cybersecurity Advisor, Geoffrey.Jenista@hq.dhs.gov
PM Kirk, Region VII Director for Infrastructure Protection, pmkirk72@hq.dhs.gov

DEVELOPED BY THE IOWA SECRETARY OF STATE

2018 Election Cybersecurity Planning Snapshot
Polk County