MINNESOTA ELECTION EMERGENCY RESPONSE GUIDE

Use this quick reference guide to aid your election emergency plan training and emergency response.

IMPORTANT CONTACT INFORMATION

Municipal Clerk: _____

County Auditor: _____

_____ : _____

Minnesota Office of the Secretary of State (MN OSS): 651-215-1440

Minnesota IT Services (MNIT): 651-201-1118

Severe Weather
RESPONSE STEPS

1. Take shelter; move voters to designated shelter areas, away from windows
2. If safe, secure ballots and voting equipment
3. If unable to shelter, get under a stable, heavy object
4. Stay away from power sources, power lines, phone lines, gas lines, and windows
5. Follow directions of emergency personnel
6. Notify your municipal clerk and/or county auditor

Violent Incident
RESPONSE STEPS

If there is violence:

- Get to a safe place and call 9-1-1
- If safe, secure ballots and voting equipment
- Follow directions of emergency personnel

Bomb threat or suspicious object:

- Act fast, keep everyone away from the object
- Call 9-1-1 and describe the threat or object

Active shooter: Run, Hide, Fight

- RUN away from the shooter
- HIDE if unable to escape
- FIGHT if needed
- Call 9-1-1 when safe

Report all incidents and suspicious activity to law enforcement, your municipal clerk, and/or county auditor.

Fire / Fire Alarm
RESPONSE STEPS

1. Evacuate the building and call 9-1-1
2. If safe, secure ballots and voting equipment
3. Take a head count and report anyone missing
4. Notify your municipal clerk and/or county auditor

Cybersecurity Incident
RED FLAGS*

- Voter lingers around voting equipment and/or attempts to tamper with the equipment
- Unusual or unauthorized activities occur on election system software
- Software operates slower than usual or frequently freezes or crashes
- Email containing long hyperlinks or attachments with no additional information
- Email from an unrecognized sender persuading you to open a link, an attachment, or scan a QR code

*List not exhaustive

Cybersecurity Incident
RESPONSE STEPS

1. Report any cybersecurity red flags to your IT, municipal clerk, and/or county auditor
2. If you suspect a device may be compromised, disconnect it from the internet and from Wi-Fi
3. Report suspicious emails to your IT to verify if suspicious emails are safe
4. If you enter information into a fraudulent website, document the information entered and change your passwords using another device and the correct website
5. Report incidents to your municipal clerk and/or county auditor