

TECHNOLOGY SUB-COMMITTEE

(Utah Democratic Party Bylaws, Article IV, Section 12. The Technology Standing Sub-committee)

The Technology Standing Sub-committee shall work with the Utah State Democratic Party Executive Committee to establish:

1. strategic goals for using technology, both at the State Party and for building the
2. technology assets the Party provides to itself, staff, campaigns, and other committees.

This sub-committee directs and manages all technology functions including:

3. data management,
4. software engineering,
5. analytics,
6. information security, and
7. project management.

1. STRATEGIC GOALS – use technology to maximize interconnection and minimize cost to the party.
 - a. Establish a standard technical framework across the state and all county organizations.
 - b. Establish a common set of software assets used across all party organizations.
2. TECHNOLOGY ASSETS – use technology to standardize a common set of software assets.
 - a. Non-personal email address for each organization to provide continuity across chairs.
 - b. Google Drive as a free backup and institutional knowledge secured using email account.
 - c. Google Calendar as a free shared event manager secured using email account.
 - d. Internet presence using email account to manage and secure website and social media.
3. DATA MANAGEMENT – use technology to simplify data management – email, directory, donation processing, free texting, unlimited cloud storage, secure online access with simple user interface.
 - a. Standardize on Breeze Database license at \$72/month.
 - b. Standardize on Microsoft Office 365 using both Teams and Zoom for video meetings.
4. SOFTWARE ENGINEERING – use technology to provide a standardized integrated platform for committees, county chairs and caucus chairs to operate from grass roots using volunteers.
 - a. Single source webpage access for all entities maintained by the Technology Committee
 - b. Single Webpage or external URL for internet presence for each party entity.
 - c. Single Google Drive folder to share volunteer files on webpage and/or social media
 - d. Single integrated shared calendar maintained and shared by each party entity.
 - e. Integrated Breeze database maintained by Technology Committee for each party entity:
 - i. Integrate donations bank processing inside webpage and/or social media.
 - ii. Integrate calendar events inside webpage and/or social media.
 - iii. Integrate unlimited free texting for each party entity.
 - iv. Provide data groupings by county, district, precinct, caucus and committee.
5. ANALYTICS – use technology to continuously monitor data to find trends, improve data accuracy.
 - a. Adopt business intelligence tools such as Zoho Analytics to analyze big data
 - i. Analyze national tools for accuracy such as VoteBuilder and ActBlue data

- ii. Analyze trends in webpage visits and social media followers and donation results.
 - b. Adopt tools like Zoho Help Desk to track problems or requests from all party entities.
 - i. Analyze trends in “help requests” to anticipate long term solutions to problems.
 - ii. Analyze trends in staff responses to requests to improve service delivery.
 - c. Perform regular audits of each entity to ensure compliance with standards and policies.
- 6. INFORMATION SECURITY – Establish a Security Policy for Utah Democratic Party as follows:
 - a. Use secure and encrypted messaging platforms for party-related communication, and exercise caution when sharing sensitive information.
 - b. Encrypt email communications and attachments containing sensitive data, use strong passwords, and enable multi-factor authentication.
 - c. Ensure Google tools are used in compliance with data handling policies, restrict access to authorized personnel, and encrypt sensitive data.
 - d. Secure websites with HTTPS, apply regular security updates, restrict website administration access, and use strong passwords and multi-factor authentication.
 - e. Handle online data, including personally identifiable information, in compliance with applicable data protection laws, limit access to authorized personnel, and encrypt sensitive data.
 - f. Establish an incident response plan, report security incidents promptly, conduct regular security audits, and provide training on security best practices.
 - g. By implementing and adhering to these guidelines, the Utah Democratic Party can enhance the security and confidentiality of messaging, email, Google tools, websites, and online data.
- 7. PROJECT MANAGEMENT – Two projects – UDP SECURITY PROJECT & COUNTY PARTY PLATFORM
 - a. UDP Security Project
 - i. STEP ONE – Distribute a survey to collect security information from all entities.
 - ii. Utah Democratic Party Computer Systems Security Breach Risk Assessment Survey

Introduction:

Thank you for participating in this survey. The purpose of this survey is to assess the risk of a security breach in the computer systems of the Utah Democratic Party. Your valuable input will help us identify potential vulnerabilities and develop strategies to mitigate the risk of a security breach. This survey consists of multiple-choice and open-ended questions. Your responses will remain anonymous and confidential.

Part 1: General Information

1. How familiar are you with computer systems and cybersecurity?

 - a) Not familiar at all
 - b) Somewhat familiar
 - c) Moderately familiar
 - d) Very familiar
 - e) Expert

2. Are you currently affiliated with the Utah Democratic Party?

 - a) Yes
 - b) No

Part 2: System Security

3. How confident are you in the overall security of the Utah Democratic Party computer systems?

 - a) Very confident
 - b) Confident
 - c) Neutral
 - d) Not confident

e) Not confident at all

4. Have you noticed any suspicious activities or potential security breaches in the past year within the Utah Democratic Party computer systems?

- a) Yes
- b) No
- c) Not sure

5. Which of the following security measures are implemented within the computer systems of the Utah Democratic Party? (Select all that apply)

- a) Firewall protection
- b) Intrusion detection system
- c) Regular software updates and patch management
- d) Antivirus and anti-malware software
- e) Encryption of sensitive data
- f) Multi-factor authentication
- g) Regular security audits and assessments
- h) User access controls and permissions
- i) Employee cybersecurity training and awareness programs
- j) Incident response plan

Part 3: Risk Assessment

6. In your opinion, which of the following factors pose the highest risk of a security breach in the Utah Democratic Party computer systems? (Rank from highest to lowest risk)

- a) Weak or easily guessable passwords
- b) Lack of regular software updates and patches
- c) Insider threats (e.g., disgruntled employees, unauthorized access)
- d) Phishing attacks and social engineering
- e) Third-party vendor vulnerabilities
- f) Inadequate employee training and awareness
- g) Insufficient physical security controls
- h) Distributed denial-of-service (DDoS) attacks
- i) Other (please specify)

7. How often are security assessments and penetration testing conducted on the Utah Democratic Party computer systems?

- a) Regularly (at least once a year)
- b) Occasionally (every 1-2 years)
- c) Rarely (every 3-5 years)
- d) Never conducted

Part 4: Recommendations

8. Based on your knowledge and experience, what additional security measures or improvements would you suggest to enhance the security of the Utah Democratic Party computer systems?

9. Are there any specific concerns or areas of vulnerability that you would like to highlight regarding the computer systems of the Utah Democratic Party?

Thank you for taking the time to complete this survey. Your input is greatly appreciated in our efforts to strengthen the security of the Utah Democratic Party computer systems.

b. COUNTY PARTY PLATFORM PROJECT

- i. STEP ONE – Informational overview of UTAHDEMS.ORG for Technology Committee by Chuck
- ii. Schedule a Zoom meeting at the convenience of the Chair and members using this Zoom account:
- iii. Join Zoom Meeting: <https://us02web.zoom.us/j/2678751687>

Respectfully proposed by Chuck Goode