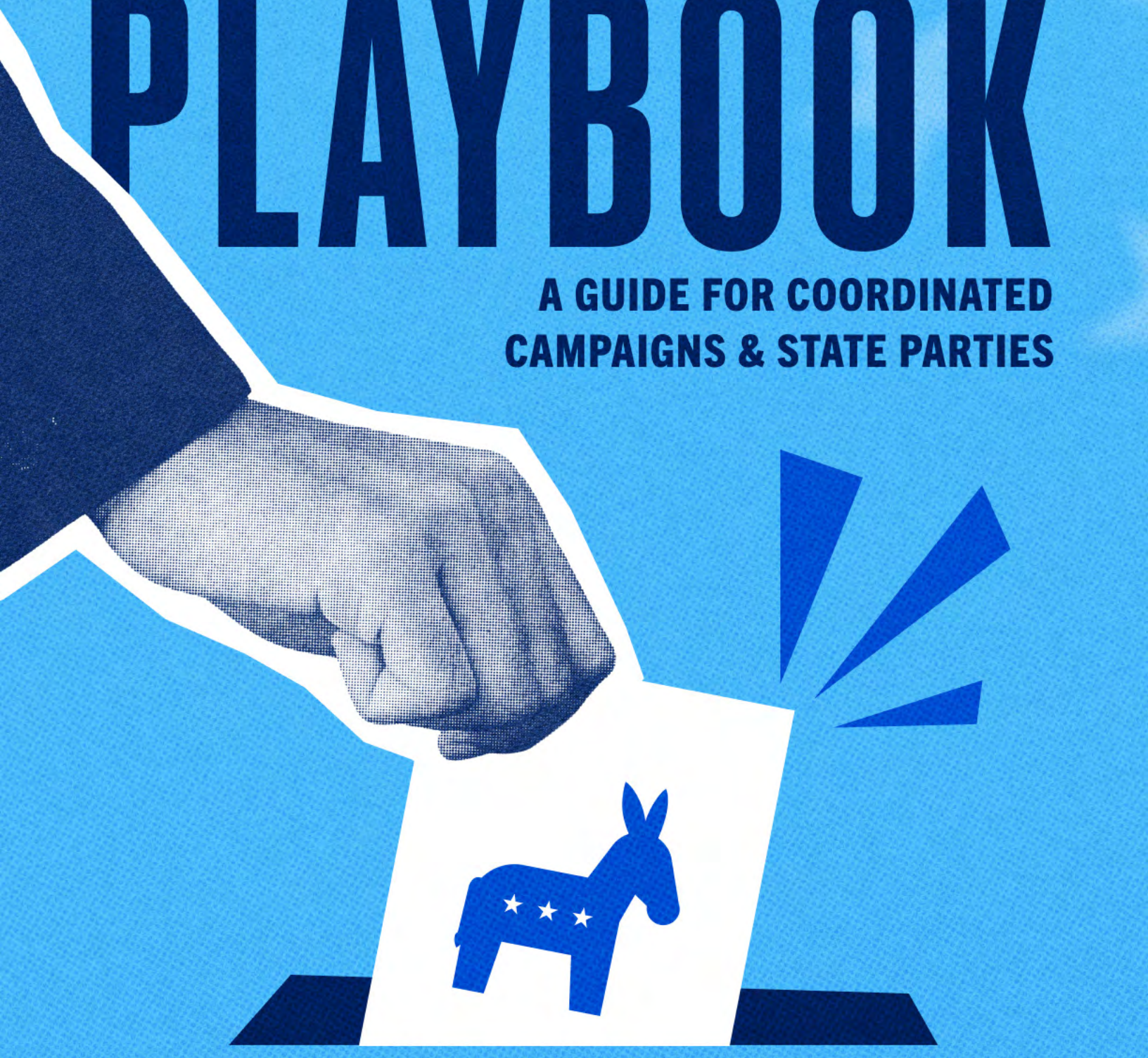
Democratic National Committee

PLAYBOOK

A GUIDE FOR COORDINATED CAMPAIGNS & STATE PARTIES



5

DEPARTMENT RESOURCES

Cybersecurity Guidance for Campaigns

Why cybersecurity matters

Campaigns are at risk of compromise from a variety of bad actors. These could be nation states disrupting our democracy, cybercriminals with financial motivation, and sometimes even people opposed to a candidate. The cost of securing your campaign is more affordable than the financial, reputational, and legal fall out of being the victim of a cyberattack.

This section of the playbook is designed to help campaigns of any size determine the best strategy for managing and reducing cybersecurity risk. Each campaign will carry different types of risk, so it is crucial to make these considerations as early as possible.

Getting Started: Threat Modeling

What is a threat model?

Threat modeling is a key part of the risk management process for organizations and campaigns, as it helps to identify potential vulnerabilities and threats before they can be exploited, allowing organizations to implement effective mitigation strategies and reduce their risk of a security breach. Consider the types of cybersecurity threats that you may face during the cycle.

Every campaign should start by asking: *what could disrupt our campaign operations, compromise our data, harm our staff or volunteers, or undermine our credibility?* From there, the campaign should identify tactical steps to reduce those risks.

When building your threat model, consider the following categories:

1. Cybersecurity threats

   Political organizations are vulnerable to cyber attacks, such as hacking and phishing, which can compromise sensitive data and harm their operations.

2. Physical threats

   Political organizations and their members can also be at risk of physical harm from extremist groups or individuals who are opposed to their beliefs and activities.

3. Financial threats

   Political organizations rely on donations and funding to support their operations, and they may face financial threats such as embezzlement or fraud.

4. Reputation threats

   Negative publicity, scandals, and controversial statements or actions can harm the reputation of political organizations and undermine their credibility.

5. Legal threats

   Political organizations may face legal challenges and investigations, such as accusations of campaign finance violations, which can result in fines or even criminal charges.

6. Electoral threats

Political organizations that participate in elections can face challenges such as voter suppression, voter intimidation, and other tactics aimed at manipulating election outcomes.

7. Internal threats

   Political organizations can also be threatened by a person who has authorized access to its systems, data, or information, such as an employee, contractor, or business partner. This person has legitimate access to the organization's resources and may use their access to intentionally or unintentionally cause harm to the organization.

Best Practices: Cybersecurity

The DNC recommends all campaigns adopt a “secure by default” approach, which means security practices are built into your operations from the beginning – not after problems occur!

Cybersecurity includes the *people* who use tools, as well as the *processes* they follow to do so. The goal is to reduce any risks of hacked accounts, data leaks, or unauthorized access to internal campaign systems.

The steps below outline how campaigns should implement core cybersecurity protections:

1. Multi-factor authentication (MFA): *Every* platform and device used by the campaign should have a form of multi-factor authentication enabled. MFA adds a powerful layer of security to your accounts — if your password is hacked or phished, this second layer of approval helps keep your accounts safe. Select the strongest form of MFA in the following priority order:
    a. Passkeys: Passkeys are an easier and more secure alternative to passwords. They let you sign into accounts with your fingerprint, face scan, or screen lock. They’re stored on your local device, and they cannot be guessed or reused.
    b. Security keys: Use security keys whenever possible because all other forms of MFA are phishable. We recommend Yubikeys and Google Titan Keys. Make sure your security keys support NFC so that you can use them with your phone. Please see the security keys section below for more details.
    c. Authenticator App: These apps generate a 6 digit code that changes every 30 seconds and verifies your identity. Google Authenticator & Duo are examples.
    d. Email: Email is only recommended if your email has MFA configured as well.
    e. SMS/text messages: Avoid SMS/text message as your MFA unless it is the only option. Ensure you have a long, random, unique password if so

2. Cybersecurity Checklist: Every new hire should complete the checklist for all of their work and personal accounts within the first week. https://democrats.org/security/

3. Password Manager: Password managers such as Keeper and 1Password help create, store, and enter login credentials for you. This additional layer of security should be required for all staff before they are given login credentials to any of your systems. Password managers, like all applications, should be secured with MFA for each user, ideally with multiple hardware security keys.

4. Passphrases versus Passwords: Create a strong master password by using a passphrase. We also recommend a passphrase for anything you have to type in frequently (like your Netflix password). Having a strong passphrase is especially important for your most critical applications, such as email and your password manager.
    a. Sample strong passphrase: *worshiper favoring visa nest*

5. Training: Cybersecurity training should be conducted at the beginning of the onboarding process. Consider hosting small group or 1:1 sessions for your highest risk individuals, especially those who are not technically proficient.
    a. [Sample Cybersecurity 101 Training Deck]

6. Security keys: Security keys should be procured for every new hire in advance of their onboarding so they can configure them when they are given login credentials to your systems. For all Federal campaign committees and some other eligible campaigns, Defending Digital Campaigns provides promo codes for Yubico Keys and Google Titan Keys through : https://defendcampaigns.org/. Please reach out to see if your campaign is eligible.

7. Vendors: As part of the Contracts process, Vendors should submit information on their cybersecurity practices for review. This process, often referred to as “Third Party Risk Management” or TPRM, is critical to ensure that the companies you entrust with your data are meeting your expectations around security.
    a. Sample: DNC’s Vendor Security Questionnaire

8. Advanced Protection: Many vendors offer some form of “Advanced Protection Plan” or “Advanced Data Protection. Examples include Google and Apple. Review what options are available for all your technology vendors, some of them may surprise you. Many ISPs have similar programs to prevent changes to Internet services, for example.

Best Practices: Device Security

At the end of the day, the most important link in the chain of protecting your campaign's data is on the phone, tablet, or computer that is used to access that information. Often covered by the generic term of "endpoint security", how you protect these devices will be critical to the success of your overall cybersecurity program.

- Keep devices up to date. In the past, it could be weeks, months, or even years between when a new vulnerability is discovered and when it becomes actively exploited by malicious actors. Today, thanks to new tools and techniques, the window has shrunk down to days, if not hours. As such, it is important that you stay on top of security patches for your equipment, and don't allow users to ignore such updates. Detailed instructions are contained in the Security Checklist.

- Enable "Find my device". All major OS vendors have the ability to track a device, so should it be stolen or otherwise "go missing" you can find it. Make sure that you have these features enabled with some central account able to track the machines (and disable them if needed). Detailed instructions are contained in the Security Checklist.

- Set a Pin. This is true on both the device as well as the mobile service provider, set a PIN. Don't allow access to the device without a password of some kind, and don't allow someone to change the mobile services for a device without a PIN of some kind. Detailed instructions are contained in the Security Checklist.

Best Practices: IT Office Setup Guidance for Campaigns

As you stand up the campaign's processes, also be thinking through offboarding and shutdown, to avoid financial and logistical ramifications. If financially feasible, it is highly recommended that the campaign provide laptops to all staff. This allows for more control over data and reduces the campaign's risk significantly.

Questions to Consider Before Finalizing Contract for Space

- What ISP (internet service provider) is already available in this building for immediate service activation?
- Is the building willing to accept packages on behalf of the leaseholder?
- Are there building access controls? Is the building locked or open to the public? Is there a front desk with a guard?

Internet Installation Day Considerations

- Ask the installation tech to help determine the best place for the router (don't put it in the basement).

- Change the password immediately after the internet is set up. Keep the internet name and password in a password manager. Do not print it and tape it to the walls.
- Confirm the firewall is activated.

What to Purchase

Router options:

- Meraki Go — less than $1,000 per office, plug-in and go
- Meraki MX75 Firewall/Router (~$600) and Meraki MR36 Wireless Access Point (~$700)
- Ubiquiti Unifi Express or Dream Router ($150-$199)

Additional equipment:

- 1GB internet speed (Coax/Broadband Connection or Fiber)
- Abode Security System (door sensors, motion sensors, cameras, keypad, 24/7 Alarm center subscription)
- Printers — Canon imageCLASS series recommended for both color and black & white
- Office Phones — Anker PowerConf for bluetooth speakerphone, or Poly Trio 8300 for VOIP

Pro Tip 💡:
The links to purchase all of these items are available in the Resource Library.

Physical Security Best Practices

Why physical security matters

Political campaigns operate in highly visible environments, and in a highly polarized political climate, staff and volunteers can be exposed to physical safety risks. Every campaign has a responsibility to prepare for these risks in advance, to ensure all staff and volunteers are protected, and to maintain the continuity of operations if an incident does occur at any point in the campaign cycle.

As such, physical security should be treated as a core responsibility of the operations function – with clear ownership and procedures shared clearly across the organization.

Organizations can follow many of the same processes, procedures, and response plans that may already exist for cybersecurity and tailor them to the physical security threat, including planning in advance and taking steps to make things harder for adversaries to succeed.

This document is meant to start a conversation and help prioritize items for your organization to address.

Assigning ownership for security planning

Every campaign, of any size, should designate a staffer responsible for overseeing physical security. The specific staffer who owns this work will depend on the size of the organization:

- Coordinated / statewide / mid-size campaigns: this security planning is typically owned by the Operations Department / Leadership teams
- Smaller campaigns: on campaigns that do not have an Operations Department, a member of the campaign leadership team should take on this responsibility, ensuring that protocols and response plans are in place.

Note: Check with your organization's leadership and legal team when creating/updating processes. These are suggestions only.

Best Practices:

- The safety and security of staff is always #1. As always, if you or your colleagues feel there is an immediate threat, please contact law enforcement immediately.
- Keep your staff contact list up-to-date. You need to make sure you have the most up to date contact information for all staff in case of an emergency.
- Identify evacuation routes and rally points for every office. Designate an office captain per office who will review all procedures with new teammates working out of the office and remind staff about protocols.
- Reiterate key procedures to staff throughout the cycle, such as the incident reporting email address and rally points. All protocols should be easily accessible by all campaign staff.

Where to start:

- Talk to your organization's leadership about physical security and emergency preparedness, including the following key items:
    - Create your Incident Response Team (IRT) *(typically: Leadership, Operations Director, Communications Director, IT Director)* and keep their contact info readily accessible
    - Create a Threats Reporting Process. All teams should be trained to report threats and safety concerns to a designated threats email in addition to alerting the security/leadership team.
    - Create an Incident Report Form template to be used in case of an incident, for the purposes of documenting the incident, police report #s and actions taken
    - Set a "rally point" outside each office, where staff should gather, so you can easily locate them
    - Train/talk to staff about emergency preparedness and incident protocols/procedures
    - Test your new processes, especially with members of the IRT, to ensure everything is working properly and get IRT team members familiar with the process

- Establish Office Captains
    - An office captain is an individual designated to be in control of an emergency in their office or area of responsibility. The main purpose of this group is the safe removal of assigned personnel and visitors from the emergency and away from the area, up to and including evacuating the building.

Ongoing actions

Security practices should be continually evaluated and reinforced throughout the course of a campaign. Leadership responsible for overseeing security should keep the following in mind:

- Scheduling training refreshers/reminders of emergency preparedness/incident response protocols/procedures
- Updating emergency/incident protocols when things change

Resources & References

Physical Security Guidance for Democratic Organizations	Physical Security Guidance for Democratic O...
Physical Security: Tactical Best Practices	Physical Security: Tactical Best Practices

Emergency Response Team Manual	Emergency Response Team Manual
Threats Reporting	Threats Reporting
Incident Report Form	Incident Report Form.docx
Events Security Checklist [Sample]	Events Security Checklist [Sample]

Playbook Link and Resource Library

#	Resource / Display Text	URL
1	Winnable Team	info@winnable.app
2	Openfield Team	sales@openfield.ai
3	Matchbook Team	info@indigo.engineering
4	Out Organize Team	info@outorganize.com
5	Sample Hiring Tracker	https://docs.google.com/spreadsheets/d/1OunF-WuiRpiDGbN782d56E5Ou7xEfhqI...
6	Trestle Collaborative	https://www.trestle.us/
7	Arena: Creating a Team Agreement	https://arena.run/tool/creating-a-team-agreement
8	Core Competency Rubric	Organizing Core Competency Tracker
9	Arena: Hiring Guide	https://arena.run/tool/hiring-guide
10	Arena: Applicant and Interview Tracker	https://arena.run/tool/applicant-and-interview-tracker
11	Arena: Embracing Equity & Inclusion on Campaigns	https://arena.run/tool/embracing-equity-and-inclusion-on-campaigns
12	GAIN Hiring/Interviewing Tips	https://docs.google.com/document/d/1RCy1Ddbzxtz_sqAJAdixQo_BDwqilyhLelSF...
13	DNC Local Listeners Materials	democrats.org/local-listeners.

IT, Cybersecurity & Physical Security Guidance for Campaigns

#	Resource / Display Text	URL
1	DNC Security Page	https://democrats.org/security/
2	Cybersecurity Checklist	democrats.org/security-checklist
3	Sample Cybersecurity 101 Training Deck	https://docs.google.com/presentation/d/1qywpKMm-l2M6LjHI9C02jrZeJ40TEIIi...
4	Defend Campaigns	https://defendcampaigns.org/
5	Sample: DNC's Vendor Security Questionnaire	https://docs.google.com/document/d/1_IDa67LuoXOyehPtH8bmY8Nn4rcfNfJZxJDr...
6	Meraki Go	https://www.meraki-go.com/product/meraki-go-complete/?ctry=us
7	Meraki MX75 Firewall/Router	https://meraki.cisco.com/product/security-sd-wan/small-branch/mx75/

#	Resource / Display Text	URL
8	Meraki MR36 Wireless Access Point	https://meraki.cisco.com/product/wi-fi/indoor-access-points/mr36/
9	Unifi Express	https://store.ui.com/us/en/pro/category/all-unifi-cloud-gateways/product...
10	Dream Router	https://store.ui.com/us/en/pro/category/all-unifi-cloud-gateways/product...
11	Abode Security System	https://goabode.com/
12	Xerox C310 Printer	https://www.xerox.com/en-us/office/printers/xerox-c310-printer
13	Canon imageCLASS MF753Cdw II	https://www.bestbuy.com/product/canon-imageclass-mf753cdw-ii-wireless-du...
14	Canon imageCLASS LBP646Cdw	https://www.bestbuy.com/product/canon-imageclass-lbp646cdw-wireless-dupl...
15	Canon imageCLASS D1650	https://www.bestbuy.com/product/canon-imageclass-d1650-wireless-black-an...
16	Canon imageCLASS LBP246dw	https://www.bestbuy.com/product/canon-imageclass-lbp246dw-wireless-black...
17	Anker PowerConf Speakerphone	https://www.bestbuy.com/site/anker-powerconf-bluetooth-speakerphone-conf...
18	Physical Security Guidance for Democratic Organizations	Physical Security Guidance for Democratic Organi...
19	Physical Security: Tactical Best Practices	Physical Security: Tactical Best Practices
20	Emergency Response Team Manual	Emergency Response Team Manual
21	Threats Reporting	Threats Reporting
22	Incident Report Form	Incident Report Form.docx
23	Events Security Checklist [Sample]	Events Security Checklist [Sample]
24	DNC Tech Community Support	tech-community@dnc.org
25	DNC CEVP Data and Tech Director for Tool & Documentation Access	porterd@dnc.org
26	Community Resource Site	dnctechcommunity.com

Digital and Mobilization Resources

#	Resource / Display Text	URL
1	FactPost on Twitter	http://twitter.com/factpostnews
2	FactPost on Facebook	http://facebook.com/factpost
3	FactPost on Instagram	http://instagram.com/factpostnews
4	FactPost on Bluesky	http://bsky.app/profile/factpostnews.bsky.social
5	The Democrats on Twitter	http://twitter.com/thedemocrats
6	Democrats on Facebook	http://facebook.com/democrats
7	The Democrats on Instagram	http://instagram.com/thedemocrats
8	Democrats.org	http://democrats.org
9	The Democrats on Threads	http://threads.com/@thedemocrats
10	Democrats on TikTok	http://tiktok.com/@democrats
11	Political Emails Archive	https://politicalemails.org/
12	Facebook Ads Library	https://www.facebook.com/ads/library/
13	Tech Community Email	tech-community@dnc.org
14	IWillVote.com	http://iwillvote.com
15	Relational Organizing Program & Workflow Details	https://docs.google.com/document/d/1XLeRiVvoeVgLfyf-6XfvpYqSlp31r9px1uZp...
16	Example UTM Source Code Builder	https://docs.google.com/document/d/1CMqUPJbs_6fMCqEHxvyWjl7jLZHfeWIoDM6t...
17	Example Text Campaign Tracker	https://docs.google.com/spreadsheets/d/108vIFUD1S0dgIQKIa272pg5Me2stEt2W...
18	Scale to Win Dialer Training (Virtual Phone Banks)	https://docs.google.com/presentation/d/1BOd8mXvtUZ_YHFmqOUZEcnL8aGBx2Cd2...
19	Zapier	https://zapier.com/
20	Monday.com	http://monday.com
21	Creator Partnerships Contact	reinm@dnc.org
22	Democrats on Bluesky	https://bsky.app/profile/democrats.org
23	Creator Touchpoints	Democrats.org/Creator-Signal ; Democrats.org/Creator-Clips