RoadMap

Strengthening Organizations. Advancing Social Justice.

Weathering the Storms

A Toolkit on Protecting Your Organization Against Opposition Attacks

April 2017

Table of Contents

Welcome

Introduction and Purpose

Over the last few years, we have taken note of the increasing number of social change groups reporting suspected or actual opposition attacks on their organizations and campaigns. In addition to the high-profile attacks on Casa de Maryland, LAANE, Planned Parenthood, Voces de la Frontera Worker Center and the now-defunct ACORN, there are smaller scale efforts to interfere with local, state and national progressive organizing and advocacy efforts. Unfortunately, these opposition efforts move from zero to sixty very quickly and have the potential to neutralize or completely reverse the reputation and effectiveness of essential social change efforts.

Initiated by staff at the Unitarian Universalist Veatch Program at Shelter Rock, we have launched this project, ***Weathering the Storms: How to Protect Your Organization Against Opposition Attacks.***

This project provides comprehensive information and resources through webinars, this toolkit and customized technical assistance to help groups be better prepared to face such attacks.

This toolkit is designed to accompany our two-part webinar series and will provide you with checklists, sample policies and resource materials that can help you prevent, prepare and respond to fabricated and known risks and attacks. Check back periodically as we will continue to update the toolkit and list of resources as additional information comes to our attention.

DISCLAIMER

The content of the webinars and this toolkit is solely the responsibility of Roadmap and the experts that have guided us throughout. The sample policies and recommendations should not be considered as legal advice and we encourage consultation of competent professionals before adopting any template documents.

Acknowledgments

We are extremely grateful for the support from the following foundations:

- Unitarian Universalist Veatch Program at Shelter Rock
- Surdna Foundation
- General Service Foundation
- Public Welfare Foundation
- Solidago Foundation
- Hill-Snowdon Foundation
- The Ford Foundation
- Unbound Philanthropy
- Rosenberg Foundation
- The Discount Foundation
- Common Counsel Foundation, and
- Needmor Fund

The "kitchen cabinet" consisting of Molly Schultz Hafid at UU Veatch, Robert Shull at Public Welfare Foundation, Amy Morris at Surdna Foundation, Laine Romero-Alston and Anna Wadia at the Ford Foundation were generous partners and guides to our team.

This project was the brainchild of funder/organizer extraordinaire, Molly Schultz Hafid of the Unitarian Universalist Veatch Program at Shelter Rock. We especially want to thank Molly and Braeden Lentz from the UU Veatch Program for their enthusiasm, energy, incredible behind the scenes support, for helping bring more funders and their grantees to this amazing project, and for being true collaborators every step of the way.

It took a village to pull this together! We received support from numerous organizations and individuals.

The project development team consisted of Emily Goldfarb, Mary Ochs, Jen Soriano, Meredith Gray, Alfreda Barringer, and Elsa Ríos from RoadMap, and our amazing colleagues at Camino PR, Elizabeth Toledo, Andrea Hagelgans, and Pablo Toledo. We received generous support and wise counsel from Beth Kingsley and Anne Spielberg of the law firm of Harmon, Curran, Spielberg + Eisenberg and Abby Levine and Melissa Mikesell at Alliance for Justice.

We are especially grateful to the organizational partners who shared their stories and lessons from the trenches. They included Javier Benavidez from Center for Civic Policy, Monica Sommerville of the PICO National Network, and Gustavo Torres of Casa de Maryland and more recently 9to5, New Florida New Majority, the National Network of Abortion Funds and others.

Once we started working on this project we heard from people far and wide, eager to tell their stories, share important resources, point us in the right direction. There are more individuals and groups than we can name, and some in fact prefer to remain anonymous. We would at least like to recognize the following individuals and organizations: PICO National Network, Leadership for the Common Good, Cris Doby of the CS Mott Fund, and Alliance for Justice.

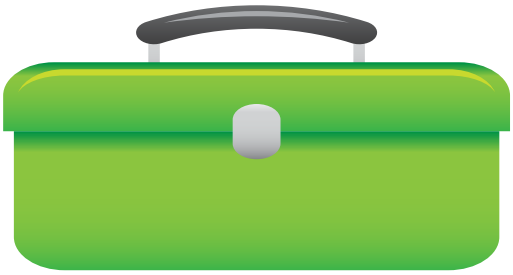
About RoadMap

RoadMap is a national network of seasoned organizational development consultants dedicated to working with social justice organizations. RoadMap is the progeny of the successful Management Assistance Program (MAP) of the French American Charitable Trust (FACT) which conducted more than 70 organizational development engagements with over 30 FACT grantees from 2004-2012, resulting in significantly improved organizational performance and outcomes. Since our spin off from FACT, RoadMap's 15 core consultants and 25+ affiliate consultants have worked with nearly 50 additional organizations using a variety of capacity building modalities.

RoadMap's overarching goal is to continue to strengthen the social justice sector by developing a range of cost-effective, capacity building services specifically tailored to the needs of social justice organizations in order to increase organizational efficacy and long-term social change impact. Please learn more about us at www.roadmapconsulting.org.

RoadMap is leading this collaborative project to serve the grantees of several foundations.

Section 1: Getting and Keeping Your House in Order



Your **TOOLKIT** items in this section include:

1.1 *Getting and Keeping Your House in Order: Our Top Twelve*
1.2 *A Guide to Getting and Keeping Your House in Order*
1.3 *Working with Funders Allies*
1.4 *Best Practices for an Ethical Organization*

Getting and Keeping Your House in Order: Our Top 12

Everything on the following checklist is important! Please review the entire document.

1. Hold regular, well-attended board meetings. Make sure minutes the document key decisions but are not too detailed.

2. Operate within your by-laws. By-laws should clearly spell out mission, including nonpartisan civic engagement & speak to term limits.

3. If you are a membership organization know and follow state requirement for membership orgs.

4. Adopt whistleblower and conflict of interest policies, as now required by IRS (990).

5. Know and stay current with all state and local registration and reporting requirements.

6. Know and follow all required employment practices. All staff should have a copy of the personnel manual and training on these policies.

7. Manage, screen and supervise all volunteers.

8. Have written fiscal policies and procedures.

9. Understand and rigorously comply with all federal, state and local lobbying documentation and reporting requirements.

10. Document steps taken to ensure that (c)3 civic engagement is nonpartisan.

11. If you have an affiliated 501(c)4 organization be sure cost sharing agreements under legal review and staff are well trained.

12. Have a Crisis Response Plan in place. Train all staff in its use and create a Crisis Management Team. The plan should clearly define delegation of roles, responsibilities, notification protocols, how to handle inquires, and messaging guidelines.

A Guide to Getting and Keeping your House in Order

This is the starting point for implementing the practices necessary to protect your organization against opposition attacks. RoadMap has prepared this checklist to help you assess your organizational vulnerabilities as a whole, and to help you identify the concrete practices and systems you will need to have in place to ensure that your organization is prepared.

This checklist covers preparation for the two types of attacks that occur: *known risks or attacks* that take advantage of noncompliance issues, and *fabricated risks or attacks* that directly threaten the reputation of the organization and/or the safety of its staff and constituents regardless of compliance issues.

We recommend that you identify one staff person as the primary "holder" of this checklist and that at least once a year and/or when there is turn over in key positions you conduct internal reviews based on this checklist.

By discussing and sharing this check list and other security protocols with your team you can identify "weaknesses" and gaps, lift up worrisome or suspicious activities that may be taking place that you are unaware of, build confidence among your staff that everything is in order, and ensure that ongoing training is taking place. Creating frequent opportunities to increase organization-wide awareness and build reassurance will go a long way towards minimizing any risks your organization may face.

1. Governance Practices		**Risks to Watch For**	**Status at My Organization**
Board Meetings and Minutes	Regular, well-attended board meetings are conducted. Minutes document decisions and demonstrate active oversight by the board. Minutes are up-to-date, on file. Minutes are distributed to all board members in a packet before the next board meeting and minutes are approved during the board meeting.	Lack of board minutes comes up in audits or legal challenges. Minutes reflect whether or not you have an engaged board, which can be the first flag someone might look for. Minutes are also important when the board itself has disputes over actions.	
Articles of Incorporation & By-Laws	Organization has articles of incorporation & bylaws and any amendments on file. Bylaws clearly state mission of the organization including nonpartisan civic engagement work and speak to term limits. Board members are familiar with and have copies of articles of incorporation and bylaws.	Overly complex bylaws can lead to problems or confusion in following proper process. Out-of-date or not following bylaws indicate lack of compliance	

1. Governance Practices		Risks to Watch For	Status at My Organization
Board Members	Organization can demonstrate that board members and officers are elected in accordance with the bylaws.	Board members need training in their roles and responsibilities.	
Whistleblower, Conflict of Interest & Confidentiality Policies	Board has adopted these policies as encouraged by the IRS.		
Document Retention and Destruction	Organization has a policy in place that includes language requiring suspension of destruction in the event of legal disputes or investigations. Staff understands and follows regular filing practices; files and folder names on servers are clear. A senior staff person can answer questions and staff should do regular cleanups. Computer backups are regular and are held offsite, email records are deleted after a set period of time. Sensitive files are locked.	During legal disputes, it is crucial to manage document searches properly and not destroy records. Email and electronic records are a major weakness in many organizations. (See Litigation Hold Policy below)	
Litigation Hold Policy	Circumstances may arise where normal and routine destruction of records must be suspended in order to comply with Federal & State legal requirements as well as present future records that are involved in litigation or reasonably anticipated in foreseeable legal action.		
Annual Report to Membership	If organization is a membership corporation, it meets state requirements regarding reporting and rights of members. This usually means an annual meeting where members elect board members.	Often groups do not have defined membership lists or they are out of date.	

1. Governance Practices		Risks to Watch For	Status at My Organization
Personnel Policies	Board has approved personnel policies including procedures to assure nondiscrimination in hiring and termination decisions and in all other terms and conditions of employment and compliance with all other applicable laws, such as those concerning wage and hours and required leave.	Board members often have little orientation prior to personnel conflicts and need immediate support to understand their role and time to brush up on policies.	

2. Business Practices and Accounting Systems		Risks to Watch For	Status at My Organization
Accounting System	Meets GAAP (Generally Accepted Accounting Principles) requirements (for larger organizations). Have an external CPA or qualified financial advisor review systems not just to meet audit standards but to ensure timely reporting/filing of financial documents.	Many groups only do annual reconciliations and allocations; monthly or quarterly is preferable.	
Fiscal Policies	Organization has written fiscal policies and procedures including internal controls for handling deposits and cash.		
Internal Controls	Key separation of duties is clear to senior managers, board treasurer and accounting staff. Essential practices are followed to appropriately approve and pay bills, sign contracts, sign checks and reconcile bank statements. More than one staff person understands internal controls and how to take care of daily transactions and accounting backups.	This is a common area of weakness or inconsistencies, making the organization vulnerable to theft and fraud.	
Cash Controls	Cash donations and petty cash both need close tracking and prompt reconciliations.		

2. Business Practices and Accounting Systems		Risks to Watch For	Status at My Organization
Audit/Audit Committee	Completed for most recent fiscal year (in some states audits not required by law, but most groups over $500,000 should have an annual or biannual audit. Determine your state's requirement). Create audit committee that meets directly with auditor (or CPA providing similar service such as a review or compilation) and an independent relationship between the board or officers and legal counsel.	For example, can be helpful if once a year the board chair calls legal counsel to ask, "Is there anything new we should be aware of?" Helps keep organization aware of any potential issues of concern.	
State and Local Registration and Reporting	Know all state and local operating and registration/reporting requirements applicable to organization's tax status. Organization meets all legal requirements to operate in the state and locality(ies) e.g. business permit etc.	Late filing of required reports & registrations makes your organization an easy target to be accused of operating "illegally."	
Liability Insurance	Insurance policy in place. Other specialized insurance coverage may be advisable depending on the nature of the organization's activities.	When holding events off-site, groups may need add-ons to their general liability policy.	
Director and Officers Insurance	Insurance policy in place.	This is mostly used to pay for legal services or settlements when the organization is sued or in disputes with an employee. Does not cover unlawful acts or gross negligence by the board.	
Workers Compensation Insurance	Insurance policy in place and staff know how to respond in case of injuries or other claims.	Make sure employees are covered in all locations where they actually work.	
Unemployment Insurance	State requirement vary. Know your local, state and federal requirements regarding unemployment insurance. Most 501(c)(3) organizations are required to have this insurance.		

2. Business Practices and Accounting Systems		Risks to Watch For	Status at My Organization
Auto Insurance	Auto insurance may be needed if activities regularly involve transporting staff, volunteers or members to activities.		
Payroll Taxes	Payroll taxes are paid each pay period and payroll reports are filed quarterly and annually. Board treasurer and/or auditor verify this quarterly.	This is a common area for liability during financial crises and high penalties can be incurred.	
Information (Tax) Returns and 990s	Properly filed public disclosure version of last three 990s readily available upon request.		
Budget Process	Board approves annual budget and mid-year adjustments. Expenditures over a set amount are subject to additional approval (e.g., large contracts or liabilities over $10,000).		
Time Sheets	Must be kept in real time, completed daily/weekly and indicate lobbying vs. non-lobbying hours and (c)(3) vs. (c)(4) hours as appropriate. Also needed to track leave time etc.	Time sheets are a critical piece of defense to show that policies and practices are in place.	
Salary policy	Board approves salary scale for categories of staff positions (not by person). Board approves benefits package. Board ensures that compensation arrangements with organizational insiders (e.g., CEO, Executive Director, Board members) are reasonable, as supported by appropriate data.	Rationale for ED compensation is a question on the 990.	

3. Lobbying and Non-Partisan Advocacy		Risks to Watch For	Status at My Organization
Lobbying	Organization has system in place for tracking, documenting and reporting lobbying expenses ("H" election, plus)	Staff needs regular training in this. Timesheets must be timely and complete.	
	Staff has been trained on lobbying limits, restrictions and reporting requirements.		
	Does your state or local government require that you register as a lobbying organization? If so, is your org registered? Then, keep up on quarterly and annual filings.		
"H" Election for 501(c)(3) (IRS form 5768)	Completed / Copy on file to declare lobbying within IRS limits is strongly recommended	Accusations of exceeding lobbying limits is a common form of attack.	
Lobbying / Ballot Initiatives	Organization has reporting process in place for direct lobbying on ballot initiatives, if applicable. In some states, ballot work requires setting up a political action committee (PAC).	Lack of accurate record keeping and tracking in real time is a huge vulnerability.	
State and Local Laws	Organization has researched and understands state and laws for civic engagement work and reporting requirements; Organization is in compliance.		
Relationships with 501(c)(4)s	If affiliated with a 501(c)(4), bylaws, contracts and cost-sharing agreements have been reviewed by legal counsel when established, and all board records are kept up to date.		

3. Lobbying and Non-Partisan Advocacy		Risks to Watch For	Status at My Organization
Implementation of Cost Sharing Agreements for 501(c)(3) / (c)(4) Organizations	Cost sharing agreements are implemented and where (c)(3) pays for things up front, the (c)(4) gets billed monthly or quarterly and invoices are paid in a timely way.	Want to avoid impression that the c3 is subsidizing the c4 organization which is not allowed.	
Training for Staff and Leaders	Organization can document training provided to staff and leaders on voter registration; voter education; GOTV, etc.	Senior staff and field staff need regular training/ refreshers on these guidelines especially with turnover.	
Documentation of Process	Organization can document the steps that it takes to ensure that civic engagement work is nonpartisan	Accusations of engaging in partisan activities are a very common form of attack and can result in loss of IRS tax exempt status	
Employee Statements / Nonpartisan Statements	Employees have signed a statement confirming that they are not allowed to engage in partisan work while on duty or on behalf of the organization. Organizational policies, such as those addressing permissible outside activities, use of organizational resources and systems, and use of and references to the organization's name and the employee's affiliation, require clear separation of personal partisan work from association with the organizations.		
Public Communications	Copies of all appeals, web content and issue educational materials use consistent language around non-partisan work, lobbying and c4 advocacy work where applicable.		

4. Fundraising		Risks to Watch For	Status at My Organization
Registration and Reporting	The organization is registered and/or has obtained necessary permits to fundraise with each state and locality it is fundraising in, as required. Reporting requirements are met in a timely manner.	Lack of compliance leads to accusations of "illegal" fundraising and penalties	
Record Keeping	Organization has records of all donations; donor information is kept secure and confidential. Sample appeal letters, printed materials, and phone scripts are kept organized.		
Tax-deductible Donation Records	Organization complies with all applicable charitable contribution rules. Donors are informed if the donation is tax deductible or not and which portion is deductible. All donations are recorded and acknowledged. All donations (single or cumulatively within a tax year) of $250 or more must be acknowledged in writing, including a statement (if true) that no goods or services were provided to the donor in return for the contribution.		
Public Communications	Copies of all appeals, web content and issue educational materials use consistent language around non-partisan work, lobbying and (c)(4) advocacy work if applicable.		
Defense Fund	A small percentage of the organizational budget is set aside in the case of unforeseen emergencies, for legal assistance, communications assistance, or other support. This could also be the same as your reserves.		

5. Employment Practices		Risks to Watch For	Status at My Organization
Personnel Policies / Employee Manual	Organization provides new employee orientation. Organization also provides updated personnel policies / employee manual to all employees. Employees acknowledge receipt in writing. Policies preserve at-will employment, unless an explicit decision is made to modify it. Clear grievance procedure is spelled out. Organization documents that all staff have received policies and notice of changes. Policies periodically reviewed for compliance with current laws. Ideally, an attorney has reviewed policies. Board has approved personnel policies including procedures to assure nondiscrimination in hiring and termination decisions and in all other terms and conditions of employment and compliance with all other applicable laws, such as those concerning wage and hours and required leave.	Annual check in with an attorney regarding any changes in employment laws is recommended. A full legal review every 3-5 years in recommended.	
Employment Forms	All employment forms required by Federal, State and local government (e.g. I-9s and W-4s) are completed before adding employees to payroll. Copies are available.		
Independent Contractors	Sign contracts and get W-9 from each independent contractor. File 1099 tax reports annually.	Ensure contractors are not doing work in ways that would make them employees.	
Classification	Ensure that individuals are appropriately classified as employees or independent contractors and as exempt or nonexempt for purposes of federal and state wage and hour laws.	Improper classification of temporary, seasonal, or part-time workers. Failure to pay minimum wage or overtime. Appropriate treatment of interns.	

5. Employment Practices		Risks to Watch For	Status at My Organization
Anti-Discrimination and Anti-Harassment Policies	Organization has policies and employees have read policies. Senior staff and board have been trained on how to respond to claims/grievances.	Senior staff and board need regular training/refreshers on how to avoid inappropriate conduct and how to respond to claims/grievances.	
Confidentiality	Organization has policies and/or signed agreements with employees and contractors requiring them to keep confidential all nonpublic organizational materials and information and to return all organizational material and property on separation from employment.	Policies should protect organizational interests, but must also comply with rules allowing concerted activity of employees.	
Equipment, Internet, Email, Social Media policies	Organization has policies in place making clear its ownership of equipment, materials, and communication systems, spelling out appropriate use of those items, and disclaiming any employee expectations of privacy while using those items.	Usage of the organization's equipment by employees or volunteers for their personal communications creates risks and vulnerabilities for the organization.	
Recruitment, Selection and Hiring	Organization has developed fair, consistent and thorough hiring process. Organization carefully reviews resumes and employment applications and prepares specific interview questions focused on ability to perform the job and skills needed. Organization checks references carefully. Organization knows legal obligations about acceptable and unacceptable interview questions and reference inquiries.	Hiring the right staff is critical for program success, organizational reputation, and legal compliance. Be on the lookout for moles and individuals who will cut corners, not produce, or violate legal obligations. Be alert for leading questions or inquiries designed to entrap. Consider requiring new hires to sign confidentiality agreements and other types of statements to deter moles.	

5. Employment Practices		Risks to Watch For	Status at My Organization
Employee Training and Supervision	Make sure you can verify employees receive job orientation and appropriate training, as needed and effective supervision.		
Exit Interview	Conduct exit interview for feedback & positive closure. Be sure to use checklist & obtain keys and equipment. Be sure to change all passwords and close accounts to which exiting employee had access.		
Volunteer Management	All volunteers are screened, trained in key protocols and procedures and supervised. References of all volunteers are checked. Limit volunteers' access to sensitive files, data and information. All volunteers should sign confidentiality agreements	Volunteers or staff working with minors under age 18 may need to be fingerprinted. Refer to precautions in the Recruitment, Selection and Hiring section above.	

6. Civic Engagement Work		Risks to Watch For	Status at My Organization
Board Support	Organization has documented support of board of directors for civic engagement work. Board minutes reflect process for endorsing events, ballot propositions, etc.		
Attorney Relations	Organization has relationships or contacts with one or more attorneys familiar with (c)(3), (c)(4), labor law and crisis management.		

6. Civic Engagement Work		Risks to Watch For	Status at My Organization
Significant Donors	Organization has support from significant donors for civic engagement work. Rules are followed regarding confidentiality and proper disclosure of donors where required (990 private pages, (c)(4) donation rules, PAC rules, etc.)		
Allied Organizations	Organization has support from allies and can call on them in time of crisis.		
	Share best practices from this checklist with your allies. Consider joint training or peer learning to prevent and respond to crises.		
Volunteer Management	All volunteers are screened, trained in key protocols and procedures and supervised.	Volunteers and staff working with minors under age 18 may need to be fingerprinted. Refer to precautions in Recruitment, Selection and Hiring under Section 5 Employment.	

7. Crisis Management Planning		Risks to Watch For	Status at My Organization
Create a Crisis Management Plan / Create a Crisis Management Team	Organization has a board approved written "**Crisis Management Plan"** and team in place for crisis management and media inquiries. All staff and key volunteers are trained and have a copy of the plan, which is reviewed and updated periodically. The plan clearly designates delegation of responsibilities, notification protocols, how to handle inquiries and messaging guidelines.	Keep a copy of keys, corporate documents, software backups and passwords off-site in case of theft or fire.	
Cultivate Communication and Legal Relationships	Proactively develop relationships with knowledgeable communication, organizational development, finance and legal professionals who can help assess and implement readiness and compliance practices, and assist you in the event of an attack.		
Allied Organizations	Organization has support from allies and can call on them in time of crisis.		
	Share best practices from this checklist with your allies. Consider joint training or peer learning to prevent and respond to crises.		

8. Crisis Communications Planning		Risks to Watch For	Status at My Organization
Goals and Success Indicators	Organizations should conduct a risk assessment and prepare crisis communications plans accordingly. For most crisis communications, the overall goal is to preserve and promote the organizational brand and values while fostering accurate and contextualized public discourse.	Goals should be specific, achievable and measurable through milestones.	
Opposition Assessment	Organization has assessed credibility, allies, traditional, online and social media activity and likely next moves of opponents.	Audit broadly – opponents might not appear in familiar channels but might still have influence.	
Communications Channels	Organization understands all channels available for proactive communication and has plans for engagement across platforms.	Don't forget about newsletters, meetings or events and direct outreach.	
Audience Assessment	Organization has identified major audience groups (staff, supporters and volunteers, the media etc.)	Remember the board and major donors. Specific communication to these audiences is critical.	
Message Strategy	Organization has developed overall brand messages as well as crisis-specific messages, tailored for groups identified in audience assessment.	All messaging should align with overall crisis and organizational messaging.	
Media Strategy	Organizations should have outlined project goals and crisis communication goals. Media assessment must include current environmental factors and an issue-specific media plan.	Media strategy should align with your target audiences and communications goals; consider both proactive and reactive strategies.	

To request assistance from RoadMap contact: info@roadmapconsulting.org

Working with Funder Allies

Molly Schultz Hafid, Unitarian Universalist Veatch Program at Shelter Rock

We know from experience that when our grantees are feeling vulnerable or under attack, they are not sure whether or not they should reach out to their funders. It is understandable to be worried that funders will be nervous if a grantee is being publicly scrutinized for actions or behavior, however fairly or unfairly. We can appreciate you may be concerned that revealing areas of potential "weakness," risk or liability, could threaten your ongoing support.

While we can't speak for all funders, on behalf of our colleagues who have supported this series of webinars, we want to be good partners to our grantees. We have invested in your organizations, and that means we believe in your work and trust that you are operating with integrity and following the law. It is in our interest to ensure that your work is not interrupted by opposition attacks. For these reasons and more, we want to help make sure that your "house is in order" and that you follow the advice laid out in this toolkit.

Whether you are looking to respond to or prevent an opposition attack, please remember that one of the most important things you can do to work well with your funders is to reach out to us.

Here are a few suggested practices for working with funder allies:

Don't wait for a crisis to talk to your funders

- Proactive relationships and communication with your most aligned funders is important as you carry out your work, review areas of vulnerability and address those areas that need more attention to fortify your organization against an attack. Regular phone and email communication maintains and deepens funder relationships.
- In the event of an attack, receiving the support that you need from funders is more likely to happen if you are proactive, rather than wait until your organization in a crisis. You don't want the only time that funders hear from you to be when you are in a crisis.
- Review grant agreements and ensure that you are in compliance with how funders have asked you to list their support. Some prefer to stay anonymous while others may want you to credit their support. Some funders give general support while others are funding a specific project.
- When in doubt about specific grants and how and if a funder wants to be listed, ask your funder.

Start with your trusted funders

- With what funders are you already in good communication? Which ones understand your organization in a deeper way? When a crisis is brewing and there are initial signs of trouble, call your most trusted individual program officer(s) regardless of their possible institutional response. These are the people with whom you can be up-front and honest about what is happening.
- As for their advice. Ask them if other funders are talking about what's happening or if they have any useful information about the source of the attack. Get a sense of whether they feel this potential threat or attack merits a larger scale response as well as advice on how to talk with your other funders.

- Be prepared for this call with any information you have about the attacks as well as a list of your core funders. The funders who have sponsored the *Weathering the Storm* webinars are a good place to start.

Assess your current, recent and prospective funders list

- Make a master list of your funders, including recent past, current and prospective funders, and identify which funders are your closest funders, your largest funders and your most public supporters. If your opponents are going to follow the money, who will they find first? Identify which funders may have discretionary funding to resource the work needed to address vulnerabilities and to prepare your staff, board and volunteers in the case of an attack.
- Pay particular attention to the type of support you receive and whether it is direct support or re-granting through an intermediary. There may be people who support your work via intermediaries that are susceptible to an attack based on "guilt by association." After you have identified your top priorities and developed a plan for communication with those at the top of your list, sort out the rest based on how likely they are to understand the situation and how an attack or public attention my impact their support.

Be honest about your risk

- In order to communicate effectively with funders about a potential or existing attack, you need to be completely honest about your risk. Regularly review the checklist in this toolkit to help you honestly assess your risks and your areas of vulnerability.
- Assess other stakeholders, collaborators and supporters who may get caught up in the conflict if an attack goes public. This is an important part of the overall assessment.

Get professional help

- If you are facing an attack, *immediately* seek legal and/or communications expertise. Before you put anything in writing, consult a lawyer or a communications expert to be sure you are not putting your organization at further risk. Remember that everything is potentially public—including emails to funders.
- There are dozens of people, including RoadMap consultants, who can provide direct technical assistance, advice and expertise in the case of an attack. These individuals and organizations can help provide added capacity and expertise that will allow you to address your needs and risks.

Program officers can be good resources -- if you have a need, make an ask

- Program officers may be able to connect you with discretionary grants, referrals to legal advice, communications experts and other resources depending on particular foundations and institutions.
- Don't be shy about reaching out to your program officers!

Be diplomatic

- Be honest in your conversations with trusted funders, while at the same time diplomatic in how you write about the situation and the support you are seeking. Remember that all of your emails are essentially public, as are funder emails. Program officers will likely share your emails with supervisors, legal counsel, board members or other staff.
- Avoiding inflammatory and rhetorical language will help you to get the resources and support you need.

Be clear with your funders about how you will respond

- Be specific about what steps you are taking with your staff, board and volunteers around communication, internally and externally, in order to prepare your organization in the case of an attack.
- Funders want to know when an attack is imminent or under way, as well about the plan that you have developed to respond. As part of your plan, consider what's appropriate to share and when.

Best Practices for an Ethical Organization

The cornerstone to protecting your organization against opposition attacks is ensuring that your operations are ethical, respectable and legally inscrutable. This overview from Harmon, Curran, Spielberg, + Eisenberg offers 9 principles that can help your organization fulfill all three of these goals.

We suggest you use this overview together with the tool that follows, the "Checklist for Getting and Keeping Your House in Order". While this overview is meant to help you set an organizational culture for doing consistent maintenance work in each of the areas described, the checklist that follows gives you descriptions of the systems necessary to put these principles into practice.

Remain focused on your mission. Review it periodically with staff. Post it on the wall. In the workplace, make sure your actions are all consistent with the organization's mission. An organization's most important asset is its reputation – don't allow your team to get sidetracked.

Establish a culture of accountability and legal compliance. Emphasize a commitment to following the law and never cutting corners. Appoint a compliance officer and listen to her. Accountability begins at the very top with a consistent message.

Empower staff. All staff should be encouraged to report anything out of the ordinary – any encounter that strikes them as unsettling. Create a central repository for these reports and designate someone to review them on a regular schedule to see if any patterns emerge. Treat this feedback as valuable information and build it into training and procedures. Where a serious pattern emerges, alert other offices and/or partner organizations.

Support honest reporting of mistakes. Staff should be encouraged to self-report interactions they may have mishandled in order to allow you to gather relevant details, preserve evidence, and prepare a response if necessary.

Protect whistleblowers. Adopt and implement a policy that encourages reporting legal or ethical misconduct within the organization. Create a clear process for reporting and investigating all allegations. Promote confidentiality of reports to the extent possible, consistent with the need to conduct an appropriate investigation. Prohibit retaliation against any person making a report in good faith, whether that report was made through internal channels or to outside law enforcement.

Don't guess. There is a natural tendency to give prompt, confident answers to clients, donors, reporters, or others. Don't forget that "I don't know" or "I'd have to check on that" are sometimes good answers. If faced with a question about an unusual topic or an issue you are not familiar with, it is worth taking the time to get the answer right.

Know the laws that apply to your operations. Know the rules that apply to all organizations (e.g., no political activity for 501(c)(3)s). Also, research any special laws that apply because of your activities. Are you registering voters? Working with minors? Handling private medical or financial information? These are just some areas that trigger special legal rules.

Train staff. It is not enough that someone in the organization knows the law, all staff should be aware of the requirements that might apply to their work. Train new staff, and provide refreshers and updates to all staff periodically. Focus on understanding what the right thing to do is in any and all situations.

And do not put untrained staff in a vulnerable position. Interns, volunteers, or brand new staff should not answer questions from the public unless they are closely and consistently supervised. Create guidance documents as refreshers/reminders.

Always be alert. Do not rely on security systems, and do not assume you can trust people. Remain pleasant and helpful in all interactions, but remember to keep your guard up. Trust your intuition.

Super Prepared Organization Sample Crisis Management Plan

SPO Crisis Protocol
In the event of an incident that could be considered a crisis, employees should first think of safety. Call 911 if you or others are in danger. Once out of danger, employees should tell their immediate supervisor or the Executive Director about the incident. Immediate supervisors who are told about an incident are called upon to use their judgment if a crisis requires immediate notification of the Executive Director. If you are somewhat uncertain as to whether to report it or not we suggest you err on the side of caution and report it.

Immediate supervisors should err on the side of notifying the Executive Director.
After the Executive Director has been notified of the incident, s/he makes a decision whether to call the Crisis Management Team. If a decision is reached to call the Crisis Management Team, the Executive Director will notify the Operations Director and the Operations Director will subsequently conduct direct notifications in the following order:

- Associate Director
- Communications Director
- Chair of the Board

All members of the Crisis Management Team have a copy of SPO's Crisis Plan to rely on in such circumstances.
Once called, the members of the Crisis Management Team will set aside all other duties and place the critical incident as their top priority. It is the responsibility of each member of the Crisis Management Team to provide for an alternate individual to carry out daily assigned responsibilities in his/her absence.

Message Discipline
During the time of notification and assessment some staff may be aware that a crisis or potential crisis has occurred. It is important that staff not engage in conversations with other staff (other than your supervisor and/or members of the CMT, if asked) friends, allies etc until such time as you receive some direction/information from the CMT. We must be careful to not contribute to rumors, gossip, or spreading panic. This could unintentionally make the situation worse. Trust that the CMT will keep everyone informed, as needed, and will be creating a communications plan and strategy.

SPO's Crisis Management Team
The Crisis Management Team has been established as an administrative decision-making group to respond to critical incidents that may occur. This team is essential to identify what actions should be taken in the event of an organizational crisis and to assist with decision-making, communications flow and operational response capability.
SPO's Crisis Management Team is comprised of:

- Executive Director
- Associate Director
- Operations Director
- Communications Director
- Chair of the Board

The job of this team is to come up with a plan of action and decide who the appropriate spokesperson (s) should be in order to protect the integrity, reputation and funding of SPO.

The Crisis Management Team may also include other staff or individuals as determined by the Crisis Management Team. Examples of additional staff or individuals who could be added to the Crisis Management Team are:

- Development Director
- New Media Strategist
- Other Board Members (c4, PAC, etc.)
- Lawyer or Accountant, if the crisis warrants
- Other staff who might be able to shed light on the crisis situation

At the first meeting of the team we will designate one member who will be the "record keeper" for the team. This member will document key information during the crisis and afterward. All team members will use great care in what is written and documented especially what is communicated via email. We will not commit to writing any sensitive information or strategy information.

Situational Assessment

Once called, the Crisis Management Team will assess the situation, determine all known facts, and begin delegation of work. The following questions should be to help develop an appropriate crisis response:

1) What is known and who already knows it?
2) What immediate steps need to be taken?
3) What additional information is needed, who will get it, and when will it be available?
4) What do we think might happen next?
5) Who on staff or the Board need to be notified or involved?
6) Do we need to notify legal counsel, insurers, authorities?
7) Are there key allies or funders who should be notified and when?

In the event of a national, state or city emergency:

If there is a natural disaster/national disasters, fire, act of terrorism etc. Call your supervisor to find out the plan. Follow up with an email. During a disaster both modes of communication may be down at times. Keep your supervisor's cell number in your phone. Expect delays in communication.

Post Crisis Evaluation

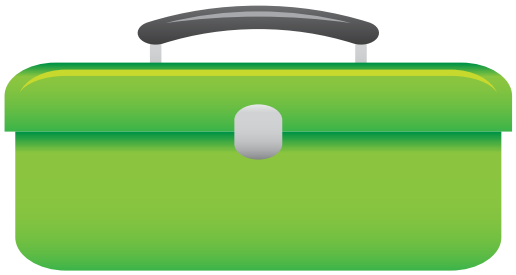
When the crisis has been resolved the CMT will meet to evaluate their management of the crisis and note lessons learned. The Crisis Plan may be adjusted based on the evaluation.

Appendix 1: Emergency Phone Tree (updated 9.9. 2013)

POSITION	NAME	PHONE NUMBER (s)
Executive Director		
Associate Director		
Operations Director		
Communications Director		

Organizer		
Board Chair		
Board Vice Chair		
Administrative Assistant		
etc.		

Section 2: Crisis Communications



Your **TOOLKIT** items in this section include:

2.1 *Crisis Communications Strategy Plan*
2.2 *Crisis Communications Risk Assessment Tool*
2.3 *Crisis Communications Knowledge Checklist*
2.4 *Crisis Communications Infrastructure Checklist*
2.5 *Crisis Communications Plan: Civic Engagement Scenario*
2.6 *Sample Social Media Policy*

Introduction

In section 1, you have the tools to gain a bird's eye view of the principles and practices needed to strengthen you overall organizational preparedness. This section will focus on communications-specific risk assessment, planning and response. Remember that communications preparation and response to opposition attacks is not just about wordsmithing the right message; it's about the internal systems and the external strategy required to both foster alignment among stakeholders and to preserve the credibility of your organization, all the while continuing to advance your mission and values in the face of an attack.

Crisis Communications Strategy Plan

Creating a written Crisis Communications Strategy Plan that addresses potential negative communications is a critical element of both preventing and managing difficult communications scenarios. Ideally, organizations will have an annual Communications Plan, and Crisis Communications Strategy Plan will be one component of that overarching strategic plan. However, even without a broad communications plan, organizations can effectively plan for difficult situations that will require an effective crisis communications strategy. This guide provided by Camino PR, will help you be prepared.

A crisis plan should have the following elements, which are detailed below:

- ✓ Goals and Success Indicators
- ✓ Opposition Assessment
- ✓ Communications Channels
- ✓ Audience Assessment
- ✓ Message Strategy
- ✓ Media Strategy- Traditional and Social Media
- ✓ Tactics and Rollout Plan

Goals

Project Goal: What are you trying to achieve with this project? Why? For example, are you trying to register unlikely voters so that the community's real needs can be reflected in an election? In most cases, the message in response to a crisis should be paired with strong messages about your charitable goal. For that reason, it's important to enumerate goals in your planning document.

Crisis Communications Goal: What is the specific goal of this communications plan? What is success? How is success measured? Generally, the primary goal of a crisis plan is to minimize the negative impact and reframe the situation with positive messaging. It is useful to indicate not only a larger goal, but also milestones. For example, minimizing the story to one day, having a brand statement included in the media coverage, etc.

Opposition Assessment

- How credible are your opponents?

- How powerful are they?
- Do they have strategic/ high-profile community allies?
- Are they frequently quoted in the media?
- Are they active in social media?
- What are their likely next moves?

Communications Channels

In what way do you currently communicate with the public? It is important to list all of the potential ways that you can proactively communicate about a crisis (including ways that others may communicate to you) and plan for how you are engaging these channels. Usually this includes:

- Online properties (website, Facebook)
- Newsletter, e-newsletter, action alerts
- Blog or Twitter feed
- Meetings or events
- Canvassing, phone banks, other direct outreach
- Advertising/marketing
- Brochures, flyers, etc.
- Media outreach (press releases and other communications)
- Direct outreach in-person, by phone, or by email to high priority constituencies such as board members and elected officials

Primary Audiences

- You'll want to identify a specific plan for each major audience type. For example, communications with board members, elected officials, and the media may require three different (though coordinated) written products.
- Internal, e.g. staff, board, advisors
- External, e.g. supporters, volunteers
- Note: Internal communications should align closely with external communications in case materials inadvertently become public.

Messages and Media Strategy

- What information will be shared?
- What is the headline? What are the 1-3 supporting points?
- What messages will you use?
- What data will you use?
- Which messengers will you use? Internal? Third party validators?

Media Assessment and Media Strategy

- Are you attempting to avoid media or manage an existing media story?
- How newsworthy is the issue and in what likely outlets?
- Who are your best media outlets and amplifiers?
- What strategies will you use for interacting with the media?
- What is the current media landscape vis a vis your issues?
- Targeted reporter list – who will be interested in this story?
- Spokesperson – who will be the public face/voice for your organization?

Tactics

Rollout plan with assignments – who is playing what part? Includes a "tick-tock" of coordinated schedules. Includes consideration of:

- Media tactics – an exclusive? A media release? Interviews? A response only? Setting the groundwork?
- Shaping the media story – using new media? Using backgrounders? Using experts? Social media engagement? Opinion outlets?
- Communicating with allies – letters to constituents? Communication with donors? Communication with staff and volunteers?

Crisis Communications Risk Assessment Tool

This communications-focused risk assessment tool contains a series of questions to help you consider all of the foreseeable risks related to your activities so that you can put prevention measures in place. There are two types of risks: known risks, and fabricated risks. This tool will help you assess the types of risks you may face, the processes you have in place to respond, and areas in which you may need to build capacity.

Known Risks

High, medium, or low risks, i.e. adverse constituent related incidents, unforeseen employee situations, volunteers not following protocol, etc. These types of risks can be more easily put into context.

- Do you have written protocols, training processes and policies that address each of these areas?
- Have legal experts reviewed your processes and policies?
- Have you trained staff and volunteers in processes?
- Do you have quality assurance protocols in place?
- Do you have a system in place for reporting potential activity by opponents?
- Have you identified a crisis management team?
- Do you have institutional (brand) messages in place?
- Do you have programmatic messages in place?
- Are your spokespersons trained in media and presentation skills?
- Do you have industry and issue specific data that puts your work in context?
- Do you have third party validators that can speak to your credibility and quality of work?
- Do you have professional communications staff and/or a professional communications consultant? Are you under resourced to the extent that you can't mobilize expertise to help respond to a crisis?
- Do you have professional staff managing your social media presence?
- How newsworthy are the issues you work on?
- How popular are the issues you work on?

Fabricated Risks

High, medium, or low risks, i.e. manipulated accusations from opponents, secret videotapes out of context, confusion regarding laws, etc.). These types of risks generally require a more rigorous communications strategy and the public needs to understand the accusations or activities in context. In addition to above, you should:

- Assess the accusations – is there any validity to any of the claims?
- Close the gaps – is there anything that needs to be corrected, i.e. staff retraining?
- Identify context – what information will help the public understand the situation?
- Messages and message map identified
- Media assessment and monitoring – what is the media worthiness of this story? What is happening on social media?

Public Reputation: How strong is your organization's public reputation? Strong, Neutral (not much presence), Negative? These are some proactive ways to measure your reputation:

- Being a regular source for expert media comment.
- Having a social media presence (Facebook followers, Twitter fans, other).
- Building a sizeable email alert list.
- Developing solid relationships with elected officials and community leaders.
- Having a positive presence in the community (events, fairs).
- What misperceptions about your work currently exist? What might your audience currently know?
- Is the value of your work a hard narrative to sell?

Brand Toolkit: What are the ways that you are proactively strengthening your reputation?

- Compelling personal stories about your work.
- Access to polling.
- Ability to jump in to media opportunities rather than simply create news.
- Marketing and/or advertising program.
- Strong relationships with community leaders and elected officials.
- A strategic media operation including social media.
- Regular communication with allies and influential people.
- An informative website with regular updates.

Crisis Communications Knowledge Checklist

A good crisis communications plan includes a roadmap that anticipates one or more ways that a situation is resolved. You can use this tool to do scenario planning that allows you to prepare protocols and responses to potential attacks. You can also use this tool as a guide for responding when an attack is underway.

Even if all of the facts are not yet known, it is important to build a roadmap that uses the best information possible to identify all of the likely scenarios. In some cases, this means building more than one version of the plan. In most cases, however, all of your scenarios will lead to the same message conclusion.

The most difficult crisis communications situation is when you must change direction midstream; this is why you must invest in building a roadmap.

Building a roadmap can feel like a maze, but with a few key questions, you can begin to understand what you know, and, just as important, what you still need to learn about a situation. This knowledge checklist will help you create the building blocks of your plan.

- ☐ What are all the verifiable facts? Get every fact you can, from as many sources as you can.
- ☐ What is the organization's position? Why? Is it publicly known? Will it change?
- ☐ Is your organization part of a network or alliance? Do you know if other organizations are experiencing similar attacks? It is important that you make sure that you and your allies are aligned in your response and messaging.
- ☐ How does your position align with standards and expectations in the field? For example, in a health care setting, what is the anticipated complication rate for a procedure? In an employee setting, how much turnover has occurred in recent years? In a civic engagement campaign, what is the anticipated percentage of unverifiable registrants that get turned in?
- ☐ What information can be shared publicly? What is the justification for not sharing specific information? (e.g., personnel policies, legal requirements)
- ☐ What is already public knowledge? What records/information is in the public record already? How many people know "confidential information"? Is the information truly confidential based on who has been told?
- ☐ What does the public deserve to know? Why? For example, is there a public health consequence? Will someone be harmed by not getting information?
- ☐ What are the various ways that the situation can be resolved? On what timetable? Often a story line will stay open until the issue is resolved. For difficult situations, you want to close the story loop as quickly and decisively as possible.

Crisis Communications Infrastructure Checklist

(SAMPLE TEMPLATE)
SCENARIO: CIVIC ENGAGEMENT

This tool takes you through the components of communications-related infrastructure that you can establish to make sure you don't get caught off-guard. The heart of this system of infrastructure is the people-powered crisis management team. This tool will help you establish an effective team and roles, policies and procedures that the team should be responsible for.

Management Team

☐ Designate your crisis management team (cross-divisional). Key members may include:

- Executive Director
- Board members
- Media/public relations contact
- Policy division member
- Communications / Website content manager
- Development staffer, if applicable
- Project manager
- Legal staff
- Consultant

- Determine your internal notification system — how will you keep your crisis response team informed? Daily calls?

Communications Policies

- Determine immediate goals and objective (using the information obtained in your Knowledge Checklist). Example objectives may include "Reduce impact of the story," "Keep organization out of the story," or "Launch campaign".

- Identify and develop an appropriate Crisis Communications Plan. See "Section 2.1: Crisis Communications Strategy Plan" for more information.

Spokespeople and Third-party Validators

☐ Identify (potential) external stakeholders:

- Organizational spokesperson
- Influential supporter(s)/Activist(s)
- Political allies
- Community allies

☐ Identify internal stakeholders:

- Board members
- Donors
- Coalition partners

Monitoring

☐ Establish a media and social media monitoring system:

- Designate staff and determine frequency
- Identify list of sites to monitor; include opposition sites and media outlets

Analysis and Production

☐ Establish a system for researching and fact-checking information and claims.

Messages and Brand

☐ Identify key messages. Internal and external messaging should be similar. Messages should lead with key values.

☐ Develop talking points and difficult questions and answers. Don't forget to address public perceptions and misperceptions.

☐ Develop internal and external communications. There is no one-size-fits-all list. See the inserts at right and above for Sample Communications Materials.

Sample External Communications Materials

- Press release/press statement
- Media advisory
- Visuals: signage, website images
- Website content
- Editorial board materials: pitch email, fact sheet
- Newsletter update (if appropriate)
- Supporter email blast
- Blog posts
- Template letters to the editor
- Advertising campaign (paid media)
- YouTube videos (consider engaging supporters to make their own videos

Sample Internal Communications Materials

- Staff update
- Key donor update
- Volunteer update
- Key board member update
- Funder update

Always assume these updates could be made public.

Things to Remember When Developing Your Organization's Crisis Communications Infrastructure:

- Internal communications should be framed with an eye to the external. Never assume that emails or messages distributed broadly to internal staff or stakeholders will remain confidential.

- Update online properties quickly (website, Facebook/Twitter). The public and the media will be looking for answers and guidance from your organization, even if you can only say you are looking into the situation.

- The media will write the story that is intriguing with or without you. It is sometimes best to provide an initial comment, even if you can only provide assurance that you are looking into the situation. "No comment" is a mistake.

- Don't speculate to the public or the press.

- Trust in your plan but also be flexible — crises situations often evolve.

- Engage your internal stakeholders and supporters throughout the crises to maintain their trust

- Debrief as soon as possible and evaluate lessons learned.

Sample Crisis Communications Plan: Civic Engagement Scenarios
(SAMPLE TEMPLATE)

SAMPLE Scenario: A charitable organization is accused of taking part in partisan activities not allowed under our charitable status.

Objectives: (Responsive and Pro-active goals)

1. Minimize negative coverage and emphasize that OUR ORGANIZATION has acted legally and ethically as a 501c3 organization.
2. Promote the great non-partisan work that OUR ORGANIZATION is doing to engage Latino and low-income and single women (i.e. low-propensity) voters in civic participation.

Audience: (*Whom will our communications strategy target for this scenario?)*

- Core funders
- Local residents of xx County, especially audiences who consume the media in which the false claims have arisen
- Reinforce our internal communications to staff, board, volunteers and donors

Identify Vulnerabilities: (*What are the most likely claims opponents might make?)*

- Claim that OUR ORGANIZATION has engaged in partisan activities, such as supporting a specific candidate
- Volunteers or other individuals taking part in GOTV work could act inappropriately or be accused of acting inappropriately by urging community members to vote for specific party or candidate, or by wearing a candidate button, etc.
- Accusation of Unethically collecting voter information
- Claim that we only engage voters with a particular political tendency in GOTV efforts
- Individual political activities of OUR ORGANIZATION's staff or board members indicate partisan activity (i.e., blurred line between personal and professional activities by a staff or board member)
- OUR ORGANIZATION distributes materials that indicate preference for one candidate over another based on member responses to issue-based surveys or candidate surveys.

Strategies to Minimize Vulnerabilities: (*The best way to weather an attack is to be above reproach, and to correct any errors promptly and systematically.)*

- Provide clear training for all volunteers that we are non-partisan and they cannot offer any opinions on a candidate or political party.
- Require that volunteers sign in, certifying that they have been trained on our non-partisan activities
- Include a message with all elections related communications that we are a nonpartisan organization. For example: *(OUR ORGANIZATION NAME) is a public charity that only engages in activities that are permissible under Internal Revenue Code section 501(c)(3). OUR ORGANIZATION and its agents are strictly prohibited from participating or intervening in any political campaign on behalf of or in opposition to any candidate for public office. All OUR ORGANIZATION's activities will be strictly non-partisan. In addition, OUR ORGANIZATION's activities will not be coordinated with any candidate, political party or other partisan entity.*
- Review all elections-related communications and materials with an attorney experienced in 501c3 compliance requirements

- Be sure that all staff unsubscribe from partisan list-serves from their work email and are reminded of this if they are updates and invites during election periods.
- Review our list-serve members. Remove any who have moved on to political or partisan work, including current candidates, party officials, or campaign or political committee employees.
- All employees must sign and comply with the "Employee Participation Rules for Volunteer Activities"

Talking points/messaging:

- We're a nonpartisan, 501(c)(3) organization dedicated to civic engagement. Nonpartisan civic activity, such as voter registration, is important and protected work. And is allowable for Charitable and educational groups
- We want people to vote, but as a nonpartisan organization, we don't tell people who to vote for nor do we support candidates for office.
- Our dream is for 100% of eligible citizens to be registered and 100% of eligible voters to go to the polls on Election Day.
- We work to ensure *all* citizens exercise their right to vote. We especially assist those who are underrepresented or face specific obstacles.
- Our community/county/state is stronger when everyone can add his or her voice to democracy.
- The freedom to vote and have a voice in the process is critical for the future of our community/county/state and future generations.
- Every citizen should have the opportunity to vote regardless of who they are, where they live, or their race, religion, or creed. We seek to remove obstacles and educate citizens about their rights.
- Young voters and others with less familiarity about government may not always realize how the decisions of policy makers impact their lives.
- We are excited to support young people and other less likely voters to get involved in civic engagement and community advocacy.

Crisis Communications Team: People who will be notified and coordinate response.

- Executive Director
- Board Chair
- Policy Director
- Communications Coordinator

Third Party Validators: *(Voices who can support our organization's reputation)*

- Board member XYZ and other attorney who has reviewed our materials and activities can support our claim to appropriate civic engagement work

Validating Message "In my capacity as [describe relationship to organization] I can say with the utmost confidence that our activities are entirely within legitimate use of 501c3 funds. [Organization] looks forward to continuing to do the important work of voter registration that our democracy deserves."

- Point to other spurious claims against non-profit groups where they were found to be (add examples from our local circles…)

Other validating messages: E.D. or Board spokespeople

In a case of any error committed by staff or volunteers:

Explain facts and give context: "This case was an exception and we immediately corrected the error when we became aware of it. We insist on the highest standards and always follow the law. Whenever

we become aware that these standards might not have been met, we take swift action to address the problem."
"We **don't discuss private personnel matters,** but I can tell you that ….we have corrected the error, [and reinforced our training to ensure that volunteers are clear on the kinds of work our organization does and does not do]."
Sample Response Plan & Dissemination *These are not recommendations but a set of possible ways to respond and how those communications might be disseminated. The team should always consider each case and the particular context and timing.*

Ways this scenario might come up and possible responses:

1. **An official inquiry such as letter from a state official or agency alleging a complaint:**

   Actions: Convene the Communications Team, Inform the Board, review the complaint and respond privately to the relevant agency. Legal assistance may be called on.
2. **A right-wing blog makes the accusation online**

   Actions: Convene the Communications Team. Monitor the blog and commenters: see if the accusation is picked up by other outlets. Do not respond unless media makes specific inquiries.

3. **Staff become aware that volunteers are wearing candidate buttons when at a rally**

   Actions: Convene the Volunteer Supervisor(s), review the non-partisan guidelines. Have the Supervisors remind all volunteers to remove buttons or other partisan materials. Reinforce this point at the next training. Have volunteers sign the guidelines when they get their next orientation.

Sample Social Media Policy

Key to communications preparedness is a common-sense security policy for social media. Social media requires increased sensitivity to the risks posed by these methods of communication. The risks are heightened because social media is so pervasive in our culture, because everything posted must be presumed to be permanent, because anything posted has the potential to reach large numbers of people across geographic boundaries, and because security in social media is uncertain. Also, because this type of communication can be viewed as less formal, there is an increased risk for inadvertent disclosure of confidential or proprietary information.

Social media has become part of our daily business and personal communications. Social media means any facility for online publication and commentary. These include but are not limited to:

- Social networking sites (Facebook, Google+, MySpace, LinkedIn, Foursquare)
- Video and photo sharing websites (Flickr, YouTube)
- Micro-blogging sites (Twitter)
- Blogs (including organization's blog or personal blogs, as well as comments)
- Forums and discussion boards (e.g. local discussion boards, Yahoo! Groups, Google Groups)

The core principle of (ORGANIZATION'S NAME)'s policy is that (ORGANIZATION'S NAME) staff, board members and volunteers should conduct themselves when communicating through social media according to the same standards and policies that otherwise apply to (ORGANIZATION'S NAME) personnel and board members overall.

Use of Social Media Must Comply with (ORGANIZATION'S NAME)'s Policy

Conduct through social media is subject to other (ORGANIZATION'S NAME)'s policies, including, without limitation, policies concerning the workplace environment, discrimination, harassment, email, confidentiality, employment references and verification, use of (ORGANIZATION'S NAME) electronic equipment and software.

Some examples of violating (ORGANIZATION'S NAME) policy through social media would be: a) posting or sending proprietary data or other confidential information; b) making statements that suggest (ORGANIZATION'S NAME) supports or opposes a candidate for elected office, etc.
Employees should be clear, respectful and transparent in their use of social media. They should be diligent in protecting the privacy of (ORGANIZATION'S NAME) and its employees.
Employees may not use (ORGANIZATION'S NAME)'s name in social media identities, log-on ID's and user names without prior approval from the Executive Director.

(ORGANIZATION'S NAME)'s allows incidental and occasional use of electronic resources for personal purposes. Except as authorized in advance, all employees are reminded not to log into social media for non-business related activities during work hours, or to do so in a manner that would interfere or be a distraction to the employee's work.

Additionally, (ORGANIZATION'S NAME) resources are not to be used for personal projects or outside work unrelated to (ORGANIZATION'S NAME) business, nor should employees engage in any activities

that negatively impact (ORGANIZATION'S NAME)'s telecommunication or computer information system; e.g. video streaming, online radio stations.

Absolutely no (ORGANIZATION'S NAME) resources may be used to support or oppose candidates for elected office. Further, employees may not engage in any activities which endorse, support or oppose any candidate for elected office from (ORGANIZATION'S NAME) offices or using (ORGANIZATION'S NAME) resources or equipment.

Nothing in this policy is intended to interfere with any employee's right to discuss terms and conditions of employment, or any other right protected under the National Labor Relations Act or any other applicable law.

No Expectation of Privacy

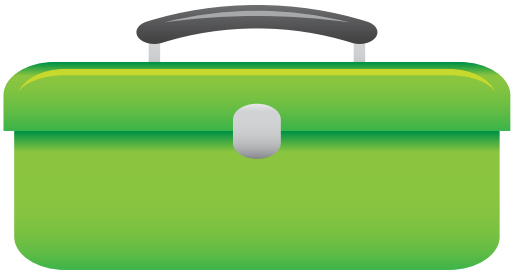
Any information on (ORGANIZATION'S NAME) electronic resources is the property of (ORGANIZATION'S NAME) and may be periodically reviewed. Employees have no expectation of privacy in connection with any information they store, send, receive, or access on (ORGANIZATION'S NAME)'s electronic resources. This includes information communicated through social media sites using (ORGANIZATION'S NAME)'s electronic resources. (ORGANIZATION'S NAME) may audit and inspect the use of its electronic resources. Likewise, (ORGANIZATION'S NAME) may monitor social media postings for legitimate, business reasons and, to the extent that postings are publicly available, employees have no expectations of privacy in such postings.

Disclaimer Language

Employees should have a disclaimer in their use of social media that their views and opinions are their own and do not represent the views of (ORGANIZATION'S NAME). As tax-exempt non-profit organization, (ORGANIZATION'S NAME) is prohibited from engaging in activities or comments that support or oppose any candidate for elected office. Employees may not engage in any activities which endorse, support or oppose any candidate for elected office from (ORGANIZATION'S NAME) offices or using (ORGANIZATION'S NAME) resources or equipment.

Accordingly, an employee should not comment in such a manner unless there was a disclaimer or the employee was not being identified as being affiliated with (ORGANIZATION'S NAME). Here is an example of appropriate disclaimer language: "The opinions expressed here are mine and not the opinions of my employer."

Section 3: Key Organizational Policies



Your **TOOLKIT** items in this section include:

3.1 *Elements of a Crisis Management Plan*
3.2 *Sample Board of Directors Conflict of Interest Policy*
3.3 *Sample Whistleblower Protection Policy*
3.4 *Sample Document Retention and Destruction Checklist*
3.5 *Corporate Attacks—Limit Your Risks*
3.6 *Volunteer Screening and Protocols*
3.7 *Sample Intern and Volunteer Questionnaire*
3.8 *Sample of Volunteer Handbook Table of Contents*
3.9 *Sample Confidentiality Agreement for Volunteers*

Introduction

In section 1, you reviewed the tools to gain a bird's eye view of the principles, policies and practices needed to strengthen your overall organizational preparedness. In section 2, you have assessment, planning, infrastructure and policy development, and a response checklist to help you implement communications-specific preparedness and response. In this section, we present a few sample tools to help you implement critical aspects of organizational compliance and common-sense security. These include sample conflict of interest and whistleblower policies, as well as guidelines for document retention and volunteer screening and management.

Sample Compliance Calendar

2017 Calendar			
January	**February**	**March**	**April**
May	**June**	**July**	**August**
State/Fed Tax Info due 5/15			8/12 Incorporated CA Annual Statement due by 31st (Sec State)
September	**October**	**November**	**December**
1st dr 2018 budget			CT-2 to AG (fundraising) 31st close of fiscal year

Below are **examples** of some of the key dates and things to note on your compliance calendar. This list is **not exhaustive** and will vary depending on your state and local requirements:

- ✓ Date/month you should begin your budget process
- ✓ Date Annual Statement of Information due (Required in most states)
- ✓ Political or Legislative Activity (lobbying) reporting or registration renewal due
- ✓ Annual information return for tax-exempt organizations (IRS 990- 990-ez or 990-N)The form must be filed on or before the 15th day of the fifth month after the close of the organization's taxable year (e.g., if the year ends December 31, the form is due no later than May 15).
- ✓ State Franchise Tax Board annual filing
- ✓ Report of fundraising activities to state and local agencies
- ✓ Board meetings (Linked to timing of budgeting, approval of IRS submission, audit etc.)

Elements of a Crisis Management Plan

☐ Notification

At the first sign of an attack or potential attacks, the Crisis Management Team (CMT) should be notified immediately. Know, in advance, what are the best means for contacting them in an emergency.

☐ Assess the Situation

- The CMT will assess the situation, determine facts, and begin delegating responsibilities.
- Consider obtaining professional help: legal, communications, or organizational support.

☐ Staff Notification

- As soon as practical, the CMT will communicate information regarding the crisis to staff.
- Include clear information and protocols for how inquiries and decisions will be handled.

☐ Board Notification

- CMT Leader alerts the Board Chair.
- Include clear information and protocols for how inquiries and decisions will be handled.
- Discuss plans and methods for informing board members and providing regular updates.

☐ Foundations and Key Partners

- CMT notifies key allies, partners, funders, etc.
- Some of these partners may need to be contacted prior to contacting the media.

☐ Message Platform

Strong messages are ones that:

- Lead with values and reflect the organization's mission
- Put information in context
- Are accurate
- Create consistency among all audiences (internal and external)

☐ Communication Strategy

- What strategies will you use for interacting with the media?
- Shaping the story
- Media rollout tactics
- Social media tactics
- Use great care regarding what is written and documented.

☐ Spokesperson Readiness

- Identify 1-2 public face/voice for your organization
- Avoid multiple spokespeople
- All spokespeople --- including those posting on social media--- must be trained on messaging
- Remember one of the top mistakes - "No Comment" or too many comments!
- Staff interviews

☐ Media and Message Evaluations

Questions to consider when monitoring media and social media (in Real Time!)

- Is the storyline escalating?
- Is it staying within the opposition or becoming "mainstream"?
- Are allies/partners engaging with supportive messaging?
- Are there supportive media outlets that could put information in context?
- Are you connecting emotionally with audiences, particularly in the social media space?
- Are there new sparks of information that warrant continued engagement?

☐ Record Keeping

- CMT designates a team member to document key information during the crisis and afterward.
- Use great care regarding what is written and documented. Use secure communications (encryption).
- Seek the advice of an attorney.

☐ Post Crisis Evaluation

- Evaluate the management of the crisis and lessons learned.

Using Your Plan

You should do at least an annual review and practice of your Crisis Management Plan. It is helpful to peg this review to something such as the first week of the New Year, "spring cleaning-first week in April" or beginning of your fiscal year, as part of your summer staff retreat etc.

When will you review your plan at least annually? _____

Make sure your plan is a part of new staff orientation, is included in your employee manual and board of director's manual. Make sure all staff and volunteers have copies.

Sample Board of Directors Minutes

Minutes for [Organization Name]

Call to Order
A [meeting type] meeting of [organization name] was held on [date] at [location]. It began at [time] and was presided over by [chairman's name], with [secretary's name] as secretary.

Attendees
Voting members in attendance include [list voting members here]
Others in attendance include [list here]
Members not in attendance included [list members who did not attend]

Approval of Minutes
A motion to approve the minutes of the previous [date] meeting was made by [name] and seconded by [name].

Reports (Financial, etc.)
[Report name] was presented by [name of presenter].
[Report name] was presented by [name of presenter].

Main Motions
Motion: Moved by [name] and seconded that [state the motion here]. The motion [carried or failed] with [number of yea's] in favor and [number of nay's] against and any abstentions.

Motion: Moved by [name] and seconded that [state the motion here]. The motion [carried or failed] with [number of yea's] in favor and [number of nay's] against and any abstentions.

Assignments

Announcements

Adjournment
[Name of mover] moved that the meeting be adjourned, and this was agreed upon at [time of adjournment].

_____ _____

Secretary
[Organization Name]

Date of Approval

Sample Board of Directors Conflict of Interest Policy

Article I: Purpose

The purpose of the conflict of interest policy is to protect the interest of (ORGANIZATION'S NAME) when it is contemplating entering into a transaction or arrangement that might benefit the private interest of an officer or director of the Organization. This policy is intended to supplement but not replace any applicable state and federal laws governing conflicts of interest applicable to nonprofit and charitable organizations.

Article II: Definitions

1. Interested Person

   Any director, member of a board committee with governing board delegated powers, or member of the staff management team (known in the personnel policies as the Management Team) who has a direct or indirect financial interest, as defined below, is an Interested Person.

2. Financial Interest

   A person has a financial interest if the person has, directly or indirectly, through business, investment, or family:

   a. An ownership or investment interest in any entity with which the Organization has a transaction or arrangement,

   b. A compensation arrangement with the Organization or with any entity or individual with which the Organization has a transaction or arrangement, or

   c. A potential ownership or investment interest in, or compensation arrangement with, any entity or individual with which the Organization is negotiating a transaction or arrangement.

   Compensation includes direct and indirect remuneration as well as gifts or favors that are not insubstantial.

   A financial interest is not necessarily a conflict of interest. Under Article III, Section 2 of this Policy, a person who has a financial interest may have a conflict of interest only if the appropriate governing board or committee decides that a conflict of interest exists.

Article III: Procedures

1. Duty to Disclose

   In connection with any actual or possible conflict of interest, an Interested Person shall disclose the existence of the financial interest and be given the opportunity to disclose all material facts to the directors and members of committees with governing board delegated powers considering the proposed transaction or arrangement.

2. Determining Whether a Conflict of Interest Exists

After disclosure of the financial interest and all material facts, and after any discussion with the Interested Person, such person shall leave the governing board or committee meeting while the determination of a conflict of interest is discussed and voted upon. The remaining board or committee members shall decide if a conflict of interest exists.

3. Procedures for Addressing the Conflict of Interest

a. An Interested Person may make a presentation at the governing board or committee meeting, but after the presentation, such person shall leave the meeting during the discussion of, and the vote on, the transaction or arrangement involving the possible conflict of interest.

b. The chairperson of the governing board or committee shall, if appropriate, appoint a disinterested person or committee to investigate alternatives to the proposed transaction or arrangement.

c. After exercising due diligence, the governing board or committee shall determine whether the Organization can obtain with reasonable efforts a more advantageous transaction or arrangement from a person or entity that would not give rise to a conflict of interest.

d. If a more advantageous transaction or arrangement is not reasonably possible under circumstances not producing a conflict of interest, the governing board or committee shall determine by a majority vote of the disinterested directors whether the transaction or arrangement is in the Organization's best interest, for its own benefit, and whether it is fair and reasonable. In conformity with the above determination it shall make its decision as to whether to enter into the transaction or arrangement.

4. Violations of the Conflicts of Interest Policy

a. If the governing board or committee has reasonable cause to believe an Interested Person has failed to disclose actual or possible conflicts of interest, it shall inform the member of the basis for such belief and afford the member an opportunity to explain the alleged failure to disclose.

b. If, after hearing the Interested Person's response and after making further investigation as warranted by the circumstances, the governing board or committee determines the Interested Person has failed to disclose an actual or possible conflict of interest, it shall take appropriate disciplinary and corrective action.

Article IV: Records of Proceedings

The minutes of the governing board and all committees with board delegated powers shall contain:

a. The names of the persons who disclosed or otherwise were found to have a financial interest in connection with an actual or possible conflict of interest, the nature of the financial interest, any action taken to determine whether a conflict of interest was present, and the governing board's or committee's decision as to whether a conflict of interest in fact

existed.

b. The names of the persons who were present for discussions and votes relating to the transaction or arrangement, the content of the discussion, including any alternatives to the proposed transaction or arrangement, and a record of any votes taken in connection with the proceedings.

Article V: Compensation

1. A voting member of the governing board who receives compensation, directly or indirectly, from the Organization for services precluded from voting on matters pertaining to that member's compensation.

2. A voting member of any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Organization for services is precluded from voting on matters pertaining to that member's compensation.

3. No voting member of the governing board or any committee whose jurisdiction includes compensation matters and who receives compensation, directly or indirectly, from the Organization, either individually or collectively, is prohibited from providing information to any committee regarding compensation.

Article VI: Statements

Each director, principal officer and member of a committee with governing board-delegated powers shall sign a statement upon assuming his/her position, which affirms such person:

a. Has received a copy of the conflicts of interest policy,

b. Has read and understands the policy,

c. Has agreed to comply with the policy, and

d. Understands the Organization is charitable and in order to maintain its federal tax exemption it shall engage primarily in activities, which accomplish one or more of its tax-exempt purposes.

Article VII: Periodic Reviews

To ensure the Organization operates in a manner consistent with charitable purposes and does not engage in activities that could jeopardize its tax-exempt status, periodic reviews shall be conducted. The periodic reviews shall, at a minimum, include the following subjects:

a. Whether compensation arrangements and benefits are reasonable, based on competent survey information, and the result of arm's length bargaining.

b. Whether partnerships, joint ventures, and arrangements with management organizations conform to the Organization's written policies, are properly recorded, reflect reasonable investment or payments for goods and services, further charitable purposes and do not result in inurement, impermissible private benefit or in an excess benefit transaction.

Article VIII: Use of Outside Experts

When conducting the periodic reviews as provided for in Article VII, the Organization may, but need not, use outside advisors. If outside experts are used, their use shall not relieve the governing board of its responsibilities for ensuring periodic reviews are conducted.

Statement by Director, Principal Officer and Member of a Committee of X

I, _____, [Interested Person] of X (the "Organization") state that:

1. I have received a copy of the conflicts of interest policy of the Organization (the "Policy").

2. I have read and I understand the Policy.

3. I agree to comply with the Policy.

4. I understand that the Organization is a charitable organization and that in order to maintain the Organization's federal tax exemption, the Organization shall engage primarily in activities, which accomplish one or more of the Organization's tax-exempt purposes.

Date: _____

By: _____

Name: _____

Title: _____

Sample Confidentiality Statement

Confidentiality Agreement of (organization name)

As an (employee, volunteer, board member) _____ of (organization name), I understand that I may be exposed to conversations, data and information/records that are considered confidential. "**Confidential Information**" includes, but is not limited to, information pertaining to financial status and operations of the organization such as organization records, strategic plans, financial reports, budget information, donations of money or gifts in kind, salary information, donors list, clients list, and personal, contact, and other information pertaining to members and clients, staff or other volunteers, oral or written and regardless of the form of communication or the manner in which it was furnished.

I acknowledge my responsibility to respect the confidentiality of (organization name), to follow (organization name) procedures in order to protect privacy, and to act in a professional manner.

I further understand that if I am found acting indiscreet with confidential material or not protecting privacy of others through my actions, I will be dismissed from my role at (organization name) immediately. I understand this action to be necessary in order to maintain high professional standards of the office and integrity of (organization name).

By signing below, I acknowledge that I have read and agree with the above policy.

Signature_____

Date_____

Signature of Supervisor or (organization name) Executive Director
_____,

_____

Date_____

Sample Confidentiality Statement (Spanish)

Declaración de Confidencialidad – MUESTRA

Acuerdo de Confidencialidad de (nombre de la organización)

Como (empleado/a, voluntario/a, miembro de la mesa directiva) _____ de (nombre de la organización), entiendo que me puedo exponer a conversaciones, datos, información y registros que se consideran confidenciales. “Información confidencial” incluye, pero no esta limitada a, información relacionada con el estatus y operaciones financieras de la organización, tales como registros de la organización, planes estratégicos, registros financieros, información del presupuesto, donativos de dinero o de servicios gratuitos, información de salarios, listas de donadores, listas de clientes, e información personal y de contacto de miembros y clientes, empleados y voluntarios, ya sea verbalmente o por escrito, sin importar la forma de comunicación o la manera por la cual fue otorgada.

Reconozco mi responsabilidad de respetar la confidencialidad de (nombre de la organización), de seguir los procedimientos de (nombre de la organización) para proteger la privacidad, y de actuar de una manera profesional.

Además, entiendo que, si actuó con una falta de discreción en cuanto a materiales confidenciales o la privacidad de los demás, me removerán de mi puesto de inmediato, con tal de mantener los estándares profesionales altos del puesto y la integridad de (nombre de la organización).

Al firmar abajo, reconozco que he leído y estoy de acuerdo con esta política.

Firma _____

Nombre (letra de molde) _____

Fecha_____

Firma del supervisor o director de (nombre de la organización)

Firma _____

Nombre (letra de molde) _____

Fecha _____

Sample Incident Report Form

(Internal Use Only)

Use this form to document safety concerns, earthquake or fire response, physical or data security breaches, injuries, theft, and suspicious situations. An incident report /near miss report should answer WHO, WHERE, WHEN, WHAT, WHY and HOW questions. [1]**Please submit a completed form to the designated incident manager and the Executive Director within 24 hours of the incident.**

ORGANIZATION NAME:_____

Name of person completing this form:	**Date form completed:**
Name of person who reported incident:	**Date of report:**
Date of incident:	**Time of incident:**
Telephone number:	**Email:**
Short description of incident:	
Area where incident occurred:	

If there was injury or potential injury, please add details and action taken
Name of injured person(s):
Injury sustained:
Immediate safety actions taken if any: (onsite first aid, emergency services/ambulance called, etc.)

Key Persons Involved/Witnesses
Name(s) and role of person(s) involved:

[1] *The reason for documenting an incident or suspicious situation or 'near miss' is to determine the cause or causes of the incident; to identify any risks, hazards, systems or procedures that contributed to the incident; and to recommend corrective action to prevent similar incidents or identify patterns. Incidents should be investigated by people knowledgeable about the type of work involved at the time of the incident. Relevant workers should also be involved in the investigation.*

Witness details Note if each person involved is a staff person, visitor, client, member, general public, person not-known. Was any person under age 18 involved or affected? If so, not age of the person		
Name/s	Job title (if relevant)	Contact number

Full description of events Describe what happened including the sequence of events, the scene of incident or near miss; who was involved; conditions present at time of incident; what was involved, what activity (if any) was taking place prior and at time of incident. What hazards was the worker exposed to? What hazards may have contributed to the incident occurring? Attach photos if available. Use more space as needed

Mandatory Notifications

The following serious incidents (known as notifiable incidents) must be immediately reported to the Executive Director and possibly to the organization's Insurer in the timeframes provided in the table below. Complete this form within 24 hours but it is not a substitute for immediate notification for serious situations.

Type of Incident	Report to:	Timeframe:	Completed Date:
Serious incidents involving a serious injury or illness of worker in the workplace or off site during work duties	Exec. Director Workers Compensation Insurance	**Immediately** **Within 48 hrs**	**Date_____** **Date_____**

Other incidents	Exec. Director	**Within 24 hrs**	**Date_____**

Comments about notification: Please note here actions taken in addition to above mandatory notifications.

Recommendations for Correction/Prevention:

Key Persons Investigating or Making recommendations to respond or prevent future incidents.
Name(s) and role of person investigating or making recommendations:

RECOMMENDATIONS e.g. new equipment, re-design work area, put in place stricter security practices, re-design work practices, review training standards, etc.

IMPLEMENTATION DETAILS including action taken, date implemented, responsible person, date for review

Sample Whistleblower Policy

This policy addresses the commitment of **(ORGANIZATION'S NAME)** to integrity and ethical behavior by helping to foster and maintain an environment where employees can act appropriately, without fear and retaliation. Employees are strongly encouraged to discuss with the executive director, other appropriate personnel, or board president when in doubt about the best and ethical course of action in a particular situation.

Reports of Wrongdoing

The company shall not take adverse employment action against an employee in retaliation for:

- Any reports or wrongdoing made in good faith; or
- Similar authority over the employee, regarding any conduct the employee in good faith believes constitutes a violation of federal law relating to fraud against the company's shareholders; or
- Participating in an investigation, hearing, court proceeding or other administrative inquiry in connection with a report of wrongdoing.

This policy is intended to encourage reporting of wrongdoing by **(ORGANIZATION'S NAME)** employees and presumes that employees will act in good faith and will not make false accusations. An employee who knowingly or recklessly makes statements or disclosures that are not in good faith may be subject to discipline, which may include termination. Employees who report acts of wrongdoing pursuant to this policy can and will continue to be held to the organization's job performance standards. Therefore, an employee against whom legitimate adverse employment actions have been taken or are proposed to be taken for reasons other than prohibited retaliatory actions, such as poor job performance or misconduct by the employee, is prohibited from using this policy as a defense against the organization's lawful actions.

For purpose of this policy:

1. Good Faith. Good Faith is evident when the report is made without malice or consideration of personal benefit and the employee has a reasonable basis to believe the report is true; provided, however, a report does not have to be proven to be true to be made in good faith. Good faith is lacking when the disclosure is known to be malicious, false or frivolous.

2. Wrongdoing. Examples of wrongdoing include, but not limited to, fraud, including financial fraud and accounting fraud, violation of laws and regulations, violations or organization policies, unethical behavior or practices, endangerment to public health or safety and negligence of duty.

3. Adverse Employment Action. Examples of adverse employment action include, but are not limited to, demotion, suspension, termination, transfer to a lesser position, denial of promotions, denial of benefits, threats, harassment, denial of compensation and privileges as a result of the employee's report of wrongdoing, or any manner of discrimination against an employee in the terms and conditions of employment because of any other lawful act done by the employee pursuant to this policy or Section 806 of the Sarbanes-Oxley Act of 2002.

Reports of Wrongdoing

An employee who becomes aware of any wrongdoing or suspected wrongdoing is encouraged to make a report as soon as possible by contacting the executive director. However, if the suspected wrongdoing involves the executive director, then the report should be made to the board president or vice president. Acts of wrongdoing may be disclosed in writing, by e-mail, by telephone or in person.

As a board member of the board of directors of **(ORGANIZATION'S NAME)** I have read this policy and agree to uphold it.

_____ _____

Signature Date

_____

Name (print)

Sample Litigation Hold Policy

Purpose

Circumstances may arise where the normal and routine destruction of records must be suspended in order to comply with Federal and State legal requirements as well as (name of organization) record retention and disposition schedules. Specifically, present and future records that are involved in litigation, or reasonably anticipated in foreseeable legal action, must be preserved until the legal hold is released by the (title of staff member authorized for this purpose. Often this would be the Executive Director, Deputy Director, Operations or Office Manager or the Legal Director)

The purpose of this document is to set forth the authority and process for initiating, implementing, monitoring, and releasing legal holds.

Scope

This policy applies to all (name of organization) staff and volunteers and covers all records made or received in the course of conducting (name of organization) business.

Definitions and Authority

"Affected Staff" means all (name of organization) staff who are in possession or control of evidence which is the subject of a legal hold.

A "legal hold" is an order to cease destruction and preserve all records related to the nature or subject of the legal hold.

"Evidence" includes all records, whether in electronic or paper form, created, received, or maintained in the transaction of (name of organization) business. Such evidence may include, but is not limited to, paper records and electronic records stored on servers, desktop or laptop hard drives, tapes, flash drives, memory sticks, or CD-ROMs.

"Electronic records" includes all forms of electronic communications, including, but not limited to, e-mail, word processing documents, calendars, spreadsheets, voice messages, videos, photographs, text messages, or information stored in PDAs.

"Staff" includes all employees and volunteers, whether permanent, temporary, full-time or part-time, contractual or on internship.

The authority to place and lift a legal hold is vested in the (title of staff position).

Procedures

I. Any (name of organization) staff member who becomes aware of any litigation, threat of litigation, other legal action, or an investigation by any administrative, civil or criminal authority, through the receipt of notification or other information identifying the possibility of legal action or upon service of a summons and complaint, must immediately notify the (title). The (title), in conjunction with other members of the Executive Team and, will determine whether to initiate a legal hold and identify staff members subject to the hold.

II. The Deputy Director will notify affected staff that a legal hold has been initiated. The notice will inform affected staff of their obligation to identify and preserve all evidence that may be relevant to the legal hold.

III. Upon notice of a legal hold, affected staff must do the following:

   A. Immediately suspend deletion, overriding, or any other destruction of electronic records relevant to the legal hold that are under their control. This includes electronic records wherever stored, including, but not limited to, on computer hard drives, flash drives, CD-ROMs, memory sticks, tapes, zip disks, diskettes, or PDAs. Electronic information must be preserved so that it can be retrieved at a later time and the information must be preserved in its original electronic form. It is not sufficient to make a hard copy. Staff is encouraged to contact the (title) with questions concerning suggested methods for preserving electronic records.

   B. Preserve any new electronic information that is generated after receipt of the legal hold notice that is relevant to the subject of the notice. This should be done by creating separate mailboxes and files and segregating all future electronically stored information into these mailboxes and files.

   C. Preserve hard copies of documents under their control. Steps should be taken to identify all relevant paper files and to ensure the retention of such files. Affected staff may make hard copies of electronically stored information; however, as specified in item (III) (A), the information must be preserved in its original electronic form.

IV. Staff subject to a legal hold must acknowledge receipt, understanding, and compliance with a legal hold without undue delay by e-mail to the (title) and their immediate supervisor. Any staff subject to a legal hold should consult (title) for assistance in securing and preserving their records.

V. The (title) will Identify all affected staff whose electronic accounts must be preserved and their status as current, former, temp, volunteer, etc. and provide all staff members information including, but not limited to official notification of the legal hold. If affected staff separate from employment during the course of a legal hold, (title i.e. Directors, supervisors etc.) must take possession of any and all evidence under the control of the separated personnel. Once notice of a legal hold has been issued, the Executive/Management Team will continue to monitor compliance with this policy and any notice.

Violations

Violation of this policy and procedure are subject to disciplinary action.

Release of a Legal Hold

The (title) will determine and communicate to affected staff when a legal hold is lifted and it is no longer necessary to preserve evidence.

Effective Date

This policy and procedures is effective _____.

Contact

Comments or questions? Please contact (title)_____.

Sample Document Retention and Destruction Policy

The corporate records of (ORGANIZATION'S NAME) are important assets. Corporate records include essentially all records you produce as an employee, whether paper or electronic. A record may be as obvious as a memorandum, an e-mail, a contract or a case study, or something not as obvious, such as a computerized desk calendar, an appointment book or an expense record.

The law requires that (ORGANIZATION'S NAME) maintain certain types of corporate records, usually for a specified period of time. Failure to retain those records for those minimum periods could subject you and (ORGANIZATION'S NAME) to penalties and fines, cause the loss of rights, obstruct justice, or spoil potential evidence in a lawsuit etc. (ORGANIZATION'S NAME) expects all employees to fully comply with any published document retention or destruction policies and schedules, provided that all employees should note the following general exception to any stated destruction schedule: If you believe, or (ORGANIZATION'S NAME) informs you, that (ORGANIZATION'S NAME) records are relevant to litigation, or potential litigation (i.e., a dispute that could result in litigation), then you must preserve those records until (ORGANIZATION'S NAME)'s Management/Directors or its legal representatives determines if the records are no longer needed. That exception supersedes any previously or subsequently established destruction schedule for those records. If you believe that exception may apply, or have any question regarding the possible applicability of that exception, please contact your supervisor or (ORGANIZATION'S NAME)'s Office Manager.

The following table provides (ORGANIZATION'S NAME) with the necessary guidance addressed by the Sarbanes-Oxley Act concerning the destruction of business records and documents

These guidelines will eliminate accidental or innocent destruction. In addition, it will provide the Executive Director with guidelines to follow when considering the length of time records should be retained.

The following table provides the minimum requirements.

Type of Document	**Minimum Requirement**
Accounts payable ledgers and schedules	7 years
Audit reports	Permanently
Bank Reconciliations	2 years
Bank statements	3 years
Checks (for important payments and purchases)	Permanently
Contracts, mortgages, notes and leases (expired)	7 years
Contracts (still in effect)	Permanently
Correspondence (general)	2 years
Correspondence (legal and important matters)	Permanently
Correspondence (with customers and vendors)	2 years
Deeds, mortgages, and bills of sale	Permanently
Depreciation Schedules	Permanently
Duplicate deposit slips	2 years
Employment applications	3 years
Expense Analyses/expense distribution schedules	7 years
Year End Financial Statements	Permanently

Insurance Policies (expired)	3 years
Insurance records, current accident reports, claims, policies, etc.	Permanently
Internal audit reports	3 years
Inventories of products, materials, and supplies	7 years
Invoices (to customers, from vendors)	7 years
Minute books, bylaws and charter	Permanently
Patents and related Papers	Permanently
Payroll records and summaries	7 years
Personnel files (terminated employees)	7 years
Retirement and pension records	Permanently
Tax returns and worksheets	Permanently
Timesheets	7 years
Trademark registrations and copyrights	Permanently
Withholding tax statements	7 years

Documents that have reached their expiration date must be destroyed within 30 days of the date unless you believe the potential litigation exception may apply (see above).

Failure to comply with this Document Retention Policy may result in punitive action against the employee, including suspension or termination. Questions about this policy should be referred to (ORGANIZATION'S NAME)'s Office Manager, who is in charge of administering, enforcing and updating this policy.

READ, UNDERSTOOD, AND AGREED:

_____ _____

Signature Date

_____

Name (print

Corporate Attacks: Limit your Risk

This tool presents some basic information about corporate attack tactics and suggests a few steps to limit your risks.

Overview

Corporate attacks on community groups and activists normally come in the form of strategic lawsuit against public participation (SLAPP) suits or via working through political allies to change laws in order to limit or counter progressive policy gains made by community groups and activists. Most corporations do not want to tarnish their image or "get their hands dirty" by engaging in direct attacks and, therefore, use lawyers, the courts and politicians to do their bidding.

A SLAPP is a lawsuit that is intended to censor, intimidate, and silence critics by burdening them with the cost of a legal defense until they abandon their criticism or opposition. Typically, SLAPP plaintiff does not normally expect to win the lawsuit. The plaintiff's goals are accomplished if the defendant succumbs to fear, intimidation, mounting legal costs or simple exhaustion and abandons the criticism. A SLAPP may also intimidate others from participating in the debate. A SLAPP is often preceded by a legal threat. SLAPPs take various forms but the most common is a civil suit for defamation. The burden is on the defendant to prove that it is not. This often includes extensive demands for "discovery" to run up the defendant's costs to respond and defend themselves.

SLAPP happy corporations sue to shut you/your organization up or to break the organization financially. This tactic has become so popular that in legal circles the name SLAPP was coined as a catchall term to describe them.

Examples of Corporate Censorship Lawsuits

Smithfield Foods used the courts to intimidate and silence those publicizing dangerous and otherwise unpleasant conditions at Smithfield's packing plant.

Smithfield filed a racketeering lawsuit against the United Food and Commercial Workers' Union (UFCW) and Jobs with Justice who were organizing workers at Smithfield's plant in Tar Heel, North Carolina. Several individuals are also named as defendants. Included among the activities which Smithfield alleged criminal were: publishing a report, passing resolutions, and speaking to the press.

Smithfield's court complaint uses the word "extort" 73 times. Some of the "unlawful" tactics alleged by Smithfield against the defendants were:

1."Publication and Use of Research Associates of America Report" (RAA was a consultant hired by UFCW to write the report).

2. "Sponsorship and Participation in the Passage of Public Condemnations of Smithfield By Cities, Townships and Organizations" (contacting elected officials and churches, asking them to pass resolutions critical of Smithfield);
3. Making “threatening statements.” A defendant "delivered the following threatening statement to Smithfield through the press: 'We’ve come here to send a message to Smithfield Foods while their board of directors and top executives gather to talk about their success and growth of the multibillion-dollar company. We want to remind them that there are people suffering every day in the largest meatpacking plant in the world.'"

Here are a few more examples that help to drive home the point home as to how cavalier these libel claims are and also to reinforce the need to be smart about public statements so as not to give your opponents any ground. It does not mean they will not sue but you do not want to minimize your risk and not give your opponents any real claim to work with.

- In Baltimore, members of a local community group faced a $52 million lawsuit after circulating a letter questioning the property-buying practices of a local housing developer.
- In Washington State, a homeowner found that she couldn't get a mortgage because her real estate company had failed to pay taxes owed on her house. She uncovered hundreds of similar cases, and the company was forced to pay hundreds of thousands of dollars in back taxes. In retaliation, it dragged her through six years of legal harassment before a jury finally found her innocent of slander.
- In Rhode Island, a resident of North Kingstown wrote a letter complaining about contamination of the local drinking water from a nearby landfill and spent the next five years defending herself against the landfill owner's attorneys, who charged her with "defamation" and "interference with prospective business contracts."

Some Guidelines to Limit Your Risks—Don’t Get SLAPPed into Submission

When you are organizing and speaking out on a matter of public controversy that involves significant corporate interests or the reputation of a government official(s), you may find yourself the target of a SLAPP. Know your rights –Limit your risks:

- Under the Constitution, you have a right to free speech and to petition the government. Courts have interpreted these rights to form legal doctrines that protect the types of activities that attract SLAPPs. Note, however, that the Constitution generally does not protect defamatory, threatening, or harassing speech.
- Tell the truth. Truth is an absolute defense to a defamation claim. You can protect yourself/your organization by not publishing rumors or scandalous innuendo, and you may want to avoid broad, sweeping generalizations or speculative rhetoric in favor of accurate, fact-based statements.

- Diligent fact-checking will make you/your organization a harder target for a SLAPP suit. Always cite to legitimate sources. Public records are an excellent source of solid factual information.
- Even if what you publish ultimately turns out not to be true, you/your organization could still have a defense if the subject of your publication is a public figure, such as a celebrity, a government official, or someone who takes on an important role in the relevant debate or controversy. Public figures must prove that you made false statements about them with "actual malice" -- that is, you actually knew that your statements were false or that you "recklessly disregarded" their falsity.
- Another common form of corporate attack employed by some corporations when they have a beef with you is to use their influence to try to cut off support and funds from the allies, funders and coalition partners. Corporations will sniff around to discover if they have ties or other means (bullying, forms of bribes=divide and conquer, intimidation) to influence your funders or your allies to question your tactics, cut off funding, speak against your organization or publicly withdraw support or membership from your organization or coalition.

This tool draws heavily on information from PR Watch a nonprofit, public interest organization dedicated to investigative reporting on the public relations industry. www.prwatch.org is a project of the Center for Media and Democracy.

Volunteer Screening and Protocol

Volunteers and interns are vital members of grassroots organizations and we depend on them! They play a critical role by assisting with multiple activities and tasks. Incorporating volunteers into our organizations is not only efficient but also an important step in overall leadership development. However, we usually don't know or screen volunteers and interns as well as we know our staff and board members. So, finding ways to give community members and leaders varying levels of responsibilities and leadership is something we want to encourage, but we need to be smart about some basic practices.

We encourage you to follow these protocols in a way that makes sense for your organization and find the right balance between your community engagement goals and "open door" practices with attention to practical security issues!

Finally, remember that we can only do our best – volunteers are not staff and thus harder to "manage"!

- Screen carefully including reference checks
- Orient and train volunteers and interns about security protocols and communication guidelines; especially important is training on what they should and shouldn't say to unfamiliar people at community meetings, through outreach activities. Make sure they know to whom to refer questions or comments or to report suspicious activities. Given them copies of important protocols and the confidentiality policy. Have them sign the confidentiality policy and also sign in at trainings.
- Use an alternative log in to computers and servers. Limit access to computers, data and servers.
- Do not allow volunteers in the office by themselves or in areas where files etc are kept. These files should be locked and volunteers should not be given keys.
- Volunteers should not have access to financial records, membership data or files, or donor records and if allowed access to your data base if must be on a restricted basis.
- If the volunteer will be working with or around minors, obtain fingerprints and a background check.
- Parental consent and/or waiver forms must be obtained prior to volunteering if the volunteer is a minor under the age of eighteen (18).

Sample Intern & Volunteer Questionnaire

ORGANIZATION NAME

Intern & Volunteer Questionnaire

OUR ORGANIZATION's MISSION is to ……INSERT TEXT HERE.

We seek volunteers for outreach and administrative work within the organization.

Volunteer Name: _____
Address: _____
Day Phone: _____ Evening Phone: _____
Email: _____

1. How many hours a week are you available to volunteer? _____
2. How long of a commitment could you make? (i.e. How many months? There is a 3-month minimum.)
_____

When could you start? _____

2. What kind of skills, talents, and / or knowledge do you think you could you use here?
_____
_____
_____

3. What kind of work might you be interested in doing for our group? Below is a list of past and possibly ongoing areas where we need volunteers, to give you an idea of the work needed. Mark ones you are interested in or suggest other projects. _____
_____

- ◊ Public Education Packets (making copies of advocacy materials, researching and preparing factsheets, etc.)
- ◊ Writing for our blog or newsletters (collect pictures, write program updates, find relevant news articles, etc.)
- ◊ Filing media archives – hard copy and electronic filing of media about our organization
- ◊ Leadership Training curriculum – updating the materials for new cohorts
- ◊ Member outreach: make calls for events, rallies, fundraising
- ◊ Event logistics: setting up/cleaning up meeting space, coordinating food, space, volunteers
- ◊ Fundraising support: Mailing donor solicitations and thank yous, collecting photos of our work
- ◊ Date base maintenance: updating addresses and emails
- ◊ Translation of written materials: In what languages are you fully bilingual? _____

4. Do you have any experience volunteering at other organizations or for other causes?
_____
_____

5. Why do you want to volunteer for our organization?

_____
_____
_____

6. What is your knowledge of the core issues we work on?

_____
_____

Please provide 2-3 references from prior employment or volunteer service.

Reference Name: _____
Relationship with Volunteer: _____
Address: _____
Day Phone: _____ Evening Phone: _____
Email: _____

Reference Name: _____
Relationship with Volunteer: _____
Address: _____
Day Phone: _____ Evening Phone: _____
Email: _____

Reference Name: _____
Relationship with Volunteer: _____
Address: _____
Day Phone: _____ Evening Phone: _____
Email: _____

(Admin: Who received inquiry: _____ Date of application: _____)

Sample of Volunteer Handbook Table of Contents

- **Organizational Overview** – Organization Mission, Org Chart, Staff Roles
- **Professionalism and Ethics** – Representing the Organization, Conflict of Interest Policy, Accepting Compensation, Gifts, Impartiality, Appropriate Use of Organization Resources
- **The Role of Volunteers** – Welcoming Volunteers From all Walks of Life, Value & Impact of Volunteers on the Lives of Those They Serve, Paid Staff vs. Volunteer Tasks
- **Workplace Safety** – Working Conditions for Volunteers, Safety Rules & Checklist, How to Handle Emergency Situations, Reporting of Accidents & Injuries, Contagious Diseases, Client Home Visit Protocol (if allowed), Suspected Abuse or Illegal Activity, Sexual Harassment & Domestic Violence, Alcohol & Drugs
- **Service Standards** – Anti-Discrimination Policy, Serving Low-Literacy & Limited-English Speaking People, Professional Boundaries & Risk Management, Liability Protections, Federal Volunteer Protection Act, State-specific Good Samaritan Law(s), Volunteer-Client Relationships, Client Confidentiality, Client Records, Serving People in Crisis
- **Supervision & Support** – Self Care, Special Accommodations, Volunteer-Paid Staff Relationships, Confidentiality of Volunteer & Staff Personal Information
- **Training Program** – Orientation and Training Course List, Peer Mentoring (If applicable), Schedule, Requirements, Certification Testing (if a highly-skilled, high risk job)
- **Supervision & Support** – Volunteer Coordinator, Other Staff, Time Sheets, Leave of Absence, Travel Reimbursement, Other Perks, Grievance and Complaint Procedure, Technology, Inclement Weather Policy
- **Volunteer Separation and Dismissal** – Resignation, Exit Interview, The Right to Progressive Discipline, Reasons for Immediate Dismissal
- **Required Reporting** – Forms, the Importance of Data Integrity, Data Submission Deadlines, Use of Agency-Approved Materials

Source:
obijohnson.typepad.com/tobisblog/2012/05/volunteer-handbooks-a-simple-guide.html

Sample Confidentiality Agreement for Volunteers

The ( ) organization requires that strict confidentiality be maintained with respect to all information obtained by volunteers concerning the organization, as well as the members, donors, and clients served. The volunteer shall not disclose any information obtained in the course of his/her volunteer placement to any third parties without prior written consent from the organization. This includes but is not limited to information pertaining to financial status and operations such as budget information, donations of money or gifts in kind, salary information, information pertaining to members and clients, staff or other volunteers.

No information concerning any volunteer will be divulged without prior written consent of the volunteer. This includes addresses, telephone numbers, etc.

Failure to comply with the confidentially policies of the organization may result in disciplinary actions, including the dismissal of the volunteer.

I understand the above and agree to uphold the confidentiality of these matters both during and following my volunteer service with the organization.

Please sign below to indicate your acceptance and agreement with these terms outlined above.

Volunteer Signature:

Date:

OR

As a volunteer of ( ) organization, I understand that I may have access to confidential information, both verbal and written, relating to members, donors, clients, volunteers or staff and the organization.

I understand, and agree, that all such information is to be treated confidentially and discussed only within the boundaries of my volunteer position at this organization.

I also agree not to discuss these same matters after I have left my volunteer position at this organization. I further understand that breach of this agreement shall constitute grounds for and may result in termination of my volunteer status with this organization.

Except where such disclosure is consistent with stated policy and relevant legislation.

Please sign below to indicate your acceptance and agreement with these terms outlined above.

Volunteer Signature:

Date:

Independent Contract definition, checklist and questions

Independent Contractor—Definition

The general rule is that an individual is an independent contractor if the person/organization paying them has the right to control or direct only the result of the work and not what, where, when it will be done and how it will be done.

You are not an independent contractor if you perform services that can be controlled by an employer (what will be done and how it will be done). This applies even if you are given freedom of action. What matters is that the employer has the legal right to control the details of how the services are performed.

For more information on determining whether you are an independent contractor or an employee, refer to the section on Independent Contractors or Employees. www.irs.gov Click on business or type independent contractor versus employee into the search bar.

Independent Contractor or Employee?

Review the following 20 questions -- a "true" independent contractor's responses appear in parenthesis following each question.

1. Are you required to comply with instructions about when, where and how the work is to be done? (No.)
2. Does your client provide you with training to enable you to perform a job in a particular method or manner? (No.)
3. Are the services you provide integrated into your client's business operation? (No.)
4. Must the services be rendered by you personally? (No.)
5. Do you have the capability to hire, supervise, or pay assistants to help you in performing the services under contract? (Yes.)
6. Is the relationship between you and the person or company you perform services for a continuing relationship? (No.)
7. Who sets the hours of work? (You do.)
8. Are you required to devote your full time to the person or company for which you perform services? (No.)
9. Do you perform the work at the place of business of the potential employer? (No.)
10. Who directs the order or sequence in which you work? (You do.)
11. Are you required to provide regular written or oral reports to your client? (No.)
12. What is the method of payment -- hourly, commission or by the job? (Fixed price, not-to-exceed, and/or milestone payments are standard for independent contractors.)
13. does the client reimburse your business and/or traveling expenses? (No.)
14. Who furnishes tools and materials used in providing services (You do. This includes workstation, internet, etc.)
15. Do you have a significant investment in facilities used to perform services? (Yes. Key here is "significant." Lots of employees have a home computer.)
16. Can you realize both a profit and a loss from your work? (Yes--very important--you must assume risk based on client satisfaction with your work.)
17. Can you work for a number of firms at the same time? (Yes.)

18. Do you make your services available to the general public? (Yes. You should have business cards, stationery, invoices and a business listing in the phone book, for example.)
19. Are you subject to dismissal for reasons other than nonperformance of contract specifications? (No.)
20. Can you terminate your relationship without incurring a liability for failure to complete a job? (No. If you work on a project or milestone basis, you must deliver to receive payment for your efforts.)

Independent Contractor Checklist

Consultant Name: _____ Program: _____

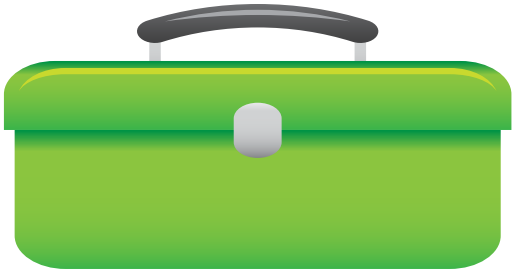
Project: _____ Contract Amt: _____

Yes/No	Required Criteria	Documentation
	This person has his/her own business and offers his/her services to the public.	Business card, website, tax ID number
	The person has other clients.	List of at least 3+ other clients.
	The work is done independently – off site and/or at the schedule of the Contractor.	
	The Contractor controls this work. The organization does not supervise or dictate how the work is done.	
	The organization does not provide instructions, directions or training about how to do the work.	
	The contractor can hire others to do the work. If assistants or sub-contractors are used, the Contractor oversees their work.	
	The Contractor has workers' comp insurance or is exempt from this requirement.	Copy of insurance or signed exemption form.
	There are not set work hours or a designated desk or office or work location office for the Contractor.	
	The relationship is established for a limited time span and does not continue indefinitely.	Written contract
	The contract does not take up all of the Contractor's work time.	
	The Contractor determines how and when to do the work.	
	There are no "interim" reports required to prove that work is being accomplished in a timely manner.	
	The Contractor is paid for the job or project, not for his/her time. The Contractor is not paid for partial work.	
	The Contractor pays for his/her usual and customary expenses.	Written contract.
	The Contractor provides his/her own tools and equipment.	Written contract.
	The Contractor cannot be fired at-will.	
	The Contractor has skills and experience pertinent to their business entity and uses initiative and/or judgment to succeed.	
	The organization and the Contractor are both clear that this is an Independent Contract relationship.	Written contract
	There is a process to hire and approve Contracts that involve more than just one person.	Written process.

Staff: _____ _____ _____

Name Signature Date

Section 4: Digital Security



Your **TOOLKIT** items in this section include background on Digital Security Readiness, a Digital Security Checklist developed by our colleagues at Information Ecology:

Digital Security in a Nutshell
Background on Digital Security for Small Organizations
Digital Security Readiness Checklist:
- *Public Wireless Use*
- *Email Protection*
- *Passwords and Authentication*

Digital Security Glossary

Digital Security in a Nutshell

Nothing digital is completely private or secret - from phone to email to texting - because it can all be monitored at "chokepoints" in the global telecommunications network. The big question for any advocacy organization is what info do we really not want to land in the hands of people who would do us harm, and who are they? Based on how we answer, we can craft a digital security strategy that balances risk with efficiency.

Here are most basic steps to the process.

1. **Threat Assessment:** Taking the time to really figure out who could do us harm, how much, and how bad is the most important step. As a small organization with all staff in the same city, and being locally rather than Federally focused, a threat assessment is fairly simple and straightforward. A few meetings and we're done.

2. **Preventative Measures:** While we are doing a threat assessment, there are very simple tools we can start practicing with now that will greatly increase our security without impacting our work (like Signal and Tor Browser). Using these tools are like washing hands – the more we do it, the easier it is to remember. And, most importantly, its preventative and saves us from the impacts of information landing in the wrong hands.

3. **Rules of Thumb for Our Stuff:** Likewise, we can also decrease doing things that are not secure, like creating easy to hack passwords or sending passwords via insecure means, like email. In general, not sending any kind of sensitive information by email is a good idea.

4. **Emergency Protocols:** in addition to washing hands, every advocacy organization should have a set of procedures in the case of digital information loss or the need to urgently communicate securely.

5. **Digital Security Strategy:** Once we've done our threat assessment, we can figure out what digital tools and procedures to prioritize beyond steps 2 – 4 above. We can implement as urgency requires but as capacity allows.

Key Concepts

End to End Encryption: This simply means that you can communicate between two people (or devices) who are both using the same encryption. Some programs or apps use encryption that is UNBREAKABLE even by national governments.

End Point Security: End point – as in, your phone, iPad or desktop. You can use the best encryption in the world to send a text, but if you lose your phone, how hard will it be to break into it? Same goes for a computer.

Open Source: Apps and programs that are made totally transparent to anyone. How can that possibly be more secure than a secret formula? It allows for public evaluation, testing, and constant improvement by digital security activists. Always choose open source programs over things that are "proprietary."

Anonymous Browsing: When you browse the internet, every computer that sees your information flowing by captures it for its own purposes. Your browser maker (Google and Microsoft) wants to know everything about you to sell you ads and the website you just landed on wants to collect as much data about who is using their site. Anonymous browsing lets you use the internet in a way that no-one knows who you are, where you are, or can track you over time.

Compartmentalizing: This means being clear and consistent about what information goes into what security bucket. For example, if we think keeping social security numbers secure is a top priority, we can create an encrypted hard drive to store them on. But that's a lot of work, and we wouldn't put everything on it. Good news – we are already doing this with Powerbase, which is highly secure, open source, and has end to end encryption. Go us!

Basic Set of Tools for Quick Digital Security

These tools work together to build an almost unbreakable flow of information when it needs to be secure. The idea is to begin practicing using them so that when the time comes to ramp up the security, we know how to use them. They are also all FREE, simple to use, and just good hygiene.

1. *Secure our direct communication* with one another using Signal. It uses end to end encryption and can be used for both texts and phone calls. It does not use your mobile provider's audio signal – it uses data signals only, which is how it can be encrypted.

2. *Use anonymous browsing* with Tor browser. You will be googling in Seattle, but other websites think you are somewhere else in the world, like Europe. AND, if you are using a website with encryption, like Google mail, your information flow can't be hacked. (Although the NSA can just ask Google for the data, but that's another story.)

3. *Use encrypted file transfer*, with Tor OnionShare or a digital activist website like riseup.net. Let's say you have a sensitive document to share. You can plop it in either a Tor browser plug-in called OnionShare or drop onto the riseup.net website, get an encryption key, then share it through Signal. (Of course, this only works if the other party has Signal!) This is a great example of compartmentalizing – we obviously don't need to do this for most of our sharing.

4. *Set up Signal on our computers* to message back and forth between Signal users on their phone or their computers. This is basically the messenger version of Signal for a desktop. We can take this to the next level by creating a special organization Signal phone number that we publish on our site and anyone can send us a totally secure message. Hello whistle blowers!

5. *Secure our devices and digital services* with better password protection. There are two steps to this. First, we have to make better passwords. Easy solution: L O N G E R is better. Second, we collect and put the passwords in a single database, on one of our computers – as well as a backup – that is encrypted. Even if our computer is stolen, the passwords can't be deciphered!

6. *Create a digital security protocol* for when staff come on board and when they leave, so that we aren't letting things fall through the cracks.

Digital Security Checklists for Small U.S. Non-Profits
by **Information Ecology**

Sections:

1) Background
2) Readiness Checklist
3) Public Wireless Use
4) Email Protection
5) Password and Authentication

What these checklists are not (and cannot be)

Effective security is an ongoing process. It requires consistent practices to be undertaken by all staff and volunteers, periodic review and adjustment to practices, and strong leadership from board and senior staff. Every organization faces a specific set of threats to its information, some of which may be completely outside the digital realm (e.g., infiltration of organizing meetings by a political adversary). As no set of checklists can address all situations, these checklists do not represent a complete solution for securing your organization.

It is also important to recognize that security and convenience are often at odds. Most security practices, both in the digital realm and the "real world", consist of trade-offs between security and efficiency. Following the checklist recommendations generally will not make your work smoother and easier. Instead, many will likely to create some disruption and training needs. In order to make meaningful strides in security, your organization must be prepared to make these trade-offs, whether steep or shallow. These investments in time and attention will repay the organization in decreased risk to critical data and systems.

How to use these checklists

The items on these checklists are meant to be actionable and accessible; each checklist item includes a brief explanation of what it means as well as, where possible, next steps for implementation. The icons accompanying each item will help you identify how difficult, disruptive and costly a given step might be to undertake.

The first checklist deals with Digital Security Readiness. If you cannot check off the items on that list, your organization should concentrate first on building the capacity to address these foundational elements before undertaking additional digital security improvements.

These checklists are part of the Weathering the Storms Getting Your House in Order Toolkit. RoadMap Consulting can offer technical assistance to work with the checklists and to integrate digital security practices into other organizational systems to protect and strengthen your organization from intrusions, political attacks, and other threats. See http://www.RoadMapConsulting.org/wts for more resources and available services.

What is digital security?

The typical technical definition of digital security says that it is the set of processes and practices used to **manage the risk** of an **adversary** exploiting **vulnerabilities** in your systems such that they may become a **threat** to the **confidentiality**, **integrity**, or **availability** of **digital assets** (e.g., file stores, cloud services, emails) or communication **channels** (e.g., instant messaging, telephone, video chats). What does that really mean? It means digital security is the work of protecting your organization's information from

being accessed, changed, or blocked by anyone—internal or external, intentionally or not—who shouldn't be able to do so. Effective security strategies, whether digital or operational, are based on the specific threats, vulnerabilities, and adversaries of your organization. This does not mean that a detailed analysis is necessary to get started improving your digital security practices. Many small U.S. organizations share a set of basic threats and vulnerabilities, which these documents are meant to help them address. (See Section: “Who these checklists are for.”)

All security practices require a **strong organizational commitment**, as they dictate changes to how you and your team work together, in addition to demanding ongoing attention to ensure that software and practices are regularly updated and working properly. The more you can understand about the threats your organization faces, the better you can select and commit to practices that will be useful for protecting your organization and its operating environment.

We have identified solutions and practices across a range of levels of technical skill and organizational commitment. The effectiveness of these practices to protect from real threats is directly correlated with the level of investment you make in implementing them. With current tools, security measures are nearly always at odds with convenience. The more you can understand what actual threats there are to your systems the more directed (and therefore less impactful to operations) your security practices will be. In this way, you assure that the more you put in to securing your systems, the more you will lower your risk of bad outcomes.

Why digital security checklists?

While computers have revolutionized how non-profits work, the last several years have begun to reveal to the general public the many risks associated with digital communication and information storage. While all organizations want to protect their information—and that of their partners and allies—few have a strong understanding of the relevant risks and most effective responses. These checklists represent recommendations for a set of baseline digital security practices. They have been created in response to incident reports, current research and community feedback about the threats faced by non-profits' computer systems, and are meant as a starting point in understanding and responding to the most basic threats computer users face today.

We offer these tools as a self-assessment guide and orientation to basic practices: we hope you find them a useful approach to help protect you and your organization from some of the serious threats that come with using computers to manage your information. Please note, they are a necessary first step to secure our movements, and are not sufficient for those of us working in extremely hostile environments, for instance against highly repressive regimes and in risky areas like conflict journalism. In no case should they be a substitute for a more aggressive security response where warranted.

Who these checklists are for

Due to the variety of threats, vulnerabilities, and adversaries that arise in different contexts of geopolitics and scale, the recommendations in these checklists apply only to organizations meeting the following criteria:

- The organization has one or more primary locations in the United States each with an office network that allows staff computers to connect to each other, internal services and the Internet. Each internal network is trusted to be free from outside interference and is segmented from the open Internet or hosting organizations' networks by a firewall device.
- The organization can successfully protect physical access to its office spaces and office network equipment.
- These office networks do not host any websites or other information resources that are meant

to be accessible to all users on the public Internet (as opposed to resources such as printers and file servers that are available only to users who are connected to the office network).
- The organization uses primarily Windows or Mac computers with some limited use of mobile devices to access its information systems.
- Although the organization may communicate with partners abroad, its staff do not cross international borders while carrying the organization's equipment or data nor regularly work in a foreign country.
- The organization is broadly seeking to protect itself from security threats from non-persistent general adversaries with limited resources (e.g., disgruntled individuals, identity thieves, political opponents, internal threats) rather than the U.S. government, other governments, or other large global entities including multinational corporations.

If these assumptions don't apply to you, these recommendations are inadequate; a more rigorous information security approach, in partnership with a provider of professional security services, is strongly recommended. Contact RoadMap for help or referrals.

Please Note: Although these practices are highly recommended they do not in and of themselves constitute a successful security practice. Information security is an ongoing process of managing risk and no list of procedures is an adequate replacement for a thorough review of what information you are protecting, why and from whom, paired with an organizational commitment to shifting operations to mitigate risk. Information Ecology, RoadMap Consulting and Common Counsel are not liable for negative outcomes associated with following these practices.

Digital Security Readiness Checklist – Baseline IT systems and practices

by ***Information Ecology***

This checklist contains baseline, ongoing information systems and technology practices that your organization must already have in place in order to successfully take on a digital security initiative. If you cannot check off more than 75% of the items in the list below, it is recommended you focus on meeting these baselines before proceeding with other digital security work. Even if at 75% or above, be sure to note the unmarked items and make plans to implement them as soon as possible, as not doing so will likely undermine your security efforts.

Readiness Assessment:

Do you have these Cultural Hallmarks for Security Success practices in place?	✔
1. Have a culture of training and learning, including strong technology training and follow-up as part of new staff orientation procedures. *New tools and practices demand end-user training. If your organization doesn't have established practices around training--when new people are hired, when refresher trainings are needed, and when important processes change--implementing improved and possibly complex secure practices is nearly impossible. Beginning with documentation and training for new hires is a wise first step in this area. Following up with new employees at 30-day intervals will ensure they continue to get the support they need to do their work effectively and securely. When a new process is introduced, it is like everyone in your organization is new to it, so initial training with similar follow-up is recommended.*	
2. Have a common and clearly communicated set of information systems that are administered by the organization and used with defined processes; ensure that all staff follow these processes effectively and are not using other systems for their work. *If your staff are using personal file-sharing, email, task management, or other accounts without knowledge or guidance from the organization, not only will your efficiency suffer but the environment becomes impractical to secure. How can you protect things you have no access to at an administrative level or, worse yet, don't even know are in use? A good place to start figuring this out if by making an inventory, collaboratively with all staff, of all the places that your information is currently stored. An important way this issue shows up in your organization is the use of cloud services. While many organizations use their personal accounts on those systems, official organizational accounts are vastly preferable. If your organization is a registered US 501c3 non-profit, most cloud providers provide licenses for their applications for free or reduced cost, providing you significant capacity to centrally manage, back up, and monitor your information at a low cost.*	
3. Have technology champions at all levels of the organization, especially leadership, and strong supervisory support and participation in systems adoption. *Leadership for technology and operations within your organization can and should come from all levels. Junior staff and younger "digital natives" on staff often use or are open to using more technology in their work so can be motivated to participate in the planning and deployment of information systems and promote uptake among peers. Of course, demonstrations of support for and engagement with technology initiatives from management are also powerful motivators for staff. Visible participation by executive leadership in training on and use of official organizational*	

Do you have these Cultural Hallmarks for Security Success practices in place?	✔
tools is a powerful modeling of preferred behavior and critical to changing organizational habits and culture.	
4. Have a complete policy set describing employees' responsibilities and limitations on their facilities, hardware, and information systems use. *Legal and operating risk due to inconsistent expectations and behavior can hamper even the most well-designed security plan. Managing your risk, employee awareness, and compliance through a strong set of workplace policies around technology but also more generally will set you up for security initiative success.*	
5. Develop and evaluate baseline non-technical security practices in an ongoing way *If you do not control your office space and access to your computers, your other digital security steps can be easily circumvented by walking into your office. Rotate alarm system codes, door codes, wireless network passwords, and other access mechanisms (for example, emergency building access plans) when staff leave the organization. Sophisticated attackers can gain full control of a computer or network with even a short period of physical access to your space or digital access to unsecured systems. More importantly, non-technical security practices help build healthy habits and a culture of security in your organization.*	

Do you have these Information Technology Operations that Support Security Outcomes practices in place?	✔
1. Have regular and adequate technical support provided either by staff assigned via job description or contracted with outside agencies. *If your existing hardware and software are not well supported, introducing new tools and practices will likely meet with significant barriers, as new technologies and tools often demand significant ongoing technical support for proper setup and functioning. There are as many ways to secure technical support as there are organizations. Talking to peer organizations in your area is a good way to find quality help.*	
2. Have a recurrent line item for technology in your budget. *Security is an ongoing process and will require ongoing investments in computer equipment and software to be effective. Work with your technical support provider to determine an appropriate amount to put into this line item.*	
3. Regardless of technical support solution, have someone on staff assigned via job description to be responsible for technical operations, including managing technical support providers and systems upgrades. *No matter how you get your technical support needs, someone needs to have time and responsibility to manage the flow of ongoing support requests, to act as a point person for vendors and consultants, and to lead projects to improve infrastructure. Although this is critical when sourcing technical support services from outside of staff to ensure your organization is owning its own operations, it is perhaps even more important when assigning technical support responsibilities to someone on staff. If internal tech support doesn't have explicit time to put into systems changes and vendor management and can only spend time fixing broken hardware and software systems, your digital security initiatives will suffer from a lack of attention.*	
4. Provide relatively new and adequately powered computers to all staff	

Do you have these Information Technology Operations that Support Security Outcomes practices in place?	✔
Industry standard best practice is to replace laptops and desktops every 3 to 5 years. Encryption tools use a lot of power and can bring older, inadequately powered computers to a near halt, making some security steps untenable for staff. Money for replacing 1/3 to 1/5 of your computers each year should be part of your recurring technology budgeting.	

Do you have these Digital Security Baseline Capacities practices in place?	✔
1. Have a process for properly onboarding and offboarding staff and volunteers that includes attention to your information systems. *The expansion or contraction of your team is a critical change in your security context, and so is an important moment to institute strong security measures. Your onboarding process should include detailed steps for the creation of accounts and instructions on how to determine and grant the correct and minimum permissions needed for that person's role. When a staff member or volunteer departs, ensure that any of the organization's data that is on their personal or work devices is copied and/or destroyed as necessary. Also at offboarding, all individual accounts belonging to the outgoing person should be deleted and any organizational passwords that they used or accessed in their work should be changed to something new.*	
2. Make sure the computers and other devices you use, including personal devices that staff may use to access organizational information, are only running the programs you expect them to by detecting and removing malware, viruses, or other intrusive software. *As a digital security first step, ensure you are running antivirus software on all computers. Antivirus software for Macs and Windows computers is available to non-profits at a discounted rate through Tech Soup. If you haven't been running antivirus software or otherwise aren't sure about the status of your devices, you can have the operating system (OS) on them reinstalled to help guarantee the computers are free of malware and viruses. This is one benefit of adopting "cloud"-based tools for your organization's information, in that your data is readily available on a freshly installed system.* *When reinstalling, use a copy from the OS provider wherever possible. Computer manufacturers often bundle other software in their installs, which may impact privacy and security but may also contain specific tools for the hardware (especially in laptops).* *Note that there are other ways in which your devices can be compromised at a level underneath the operating system; this cannot be remedied by an OS reinstall. If your computers have been handled by third parties you don't trust or out of your possession in a hostile environment, or if you suspect intrusion by powerful or well-resourced entities, get a new computer and call a security professional.*	

3. Minimize or eliminate the use of shared accounts where more than one person, especially less-vetted parties like volunteers, can log in to your systems using the same credentials. *While in the short term sharing accounts and login information can be expedient and lower licensing fees, the long-term ability to monitor and control access is more important to security outcomes. In addition, the disruption and security concerns caused by changing a broadly used password and sharing it around are potential costs that shouldn't be ignored. Sophisticated systems like GSuite or Office365 allow for "account delegation," where two people can share an account using their own distinct login credentials; this is a better way to solve these challenges than account sharing.*	
4. Have a disaster recovery plan that includes making and testing regular backups of organizational data that are stored away from your main office site. Backup drives should be at a minimum stored in a physically secure location like a locking file cabinet or safety deposit box, and ideally encrypted so that only you can access them. Do not rely exclusively on third parties to back up and hold your information. *This digital security practice is a straightforward way to protect yourself from a whole host of events that could compromise your information's integrity or cause you to lose access to it; it is so critical that it needs to come before any other digital security steps. Talk to your technical support provider about the status of your backups and when restoring data from them was last tested.*	

If you have these baseline practices in place, you are ready to improve other practices: See checklists for Email Safety, Password and Authentication Safety, and Public Wireless Network Safety.

Please Note: Although these practices are highly recommended they do not in and of themselves constitute a successful security practice. Information security is an ongoing process of managing risk and no list of procedures is an adequate replacement for a thorough review of what information you are protecting, why and from whom paired with an organizational commitment to shifting operations to mitigate risk. Information Ecology, RoadMap Consulting and Common Counsel are not liable for negative outcomes associated with following these practices.

Legend: What the icons mean

 **Stars: Overall Difficulty of the recommended practice**

This star icon represents the overall difficulty rating for a checklist item. One-star items should be doable by most technology capable organizations. Items with two stars may require some outside assistance and work flow shifts. Three stars will require significant organizational commitment of resources and technical assistance. Items with four stars are only for organizations ready to take on advanced security practices, including the ongoing commitment of human and other resources needed to make them effective.

 **Tools: Level of Technical Skill required**

This tools icon represents the amount of technical skill needed to undertake the practice. One set of tools means most skilled computer users can do, or be trained to do, the task. Two sets of tools require "power user" technical skills, often found in the "Accidental Techie" on staff. Three sets of tools will require a technical support person to do the work. Four sets of tools mean you will need a technical support person with significant skills in networking or security to undertake the practice.

 **Lightning Bolt: Time, training and work shifts required**

This lightning-bolt icon represents the amount of work flow disruption taking on this task entails, and consequently how much staff time for documentation, training and work shifts is required. One lightning bolt items will be mostly innocuous and staff can be trained in a brief session. Two lightning bolts means the practice will require more training and can disrupt existing work flows dramatically. Three lightning bolts signals that significant workflow shifts and training will be required to undertake the practice. Four lightning bolts means the task will disrupt workflow completely and is only for organizations where security is of far greater importance than efficiency or convenience.

 This checkmark icon flags columns for you to record actions you have taken. Check them off as you go!

Email Safety Checklist

This checklist provides a number of practices that can help protect you and your staff when using email to communicate. Before writing an email, ask yourself, would I put this on a postcard that might be kept forever? If the answer is no, consider using other means to communicate.

Think about email you receive like a closed envelope. If you don't know who sent it or what is in the envelope, you should open it very carefully. Especially since, in the case of email, it may contain viruses or other threats to your organization.

If performing work using sensitive or confidential information including that required to be protected by law (such as personal health information, employment records and credit card numbers) you must avoid the use of regular (non-encrypted) email to communicate that information. Where email is your only communication option, you may need to implement an encryption scheme as found in the final checklist item below.

LEGEND ✔ Record actions ★ Difficulty rating 🛠 Technical skill level 🗲 Work flow disruption

Email Safety Tasks	✔	★	🛠	🗲
1. Train people in your organization not to send sensitive or controversial information over email whenever possible. *Information in these categories includes but is not limited to credit card information, social security numbers, health information, organizational strategy, potentially damaging critiques or insults. Establish other practices for sharing this information such as instant messaging, secure downloads or plain old paper mail.*		★		🗲
2. Use strong passwords for all email accounts; change them on a regular basis, and immediately if you have any suspicion of them being used by a third party. *Strong passwords generally are made with a mix of letters, numbers and symbols and are as long as possible. Teach everyone in your organization how to generate and store strong passwords, as well as how to reset their own passwords to critical accounts. Good passwords can be made a variety of ways. One recommended method is called Diceware: http://world.std.com/~reinhold/diceware.html.*		★★	🛠🛠	🗲🗲

LEGEND ✔ Record actions ★Difficulty rating 🛠 Technical skill level 🗲Work flow disruption

Email Safety Tasks	✔	★	🛠	🗲
3. Learn to recognize suspicious behavior in your email account. *Generally, anything unexpected in your email should be looked at with suspicion. Be wary of any messages that ask you to do something, including clicking a link, opening an attachment or emailing back information. Be aware that it can be easy to fake email "From" addresses, so notice any emails that don't match the usual style of the sender indicated in the "From" address. If someone has broken into your account, you may see reply messages you don't understand, additional sent items, new folders or filters being created, or other settings changes. Suspicious emails or account behavior should be reported to a technical support person and you should preemptively change your password.*		★	🛠	🗲
4. Always login to email over a private connection. *This means using an address that starts with https:// for webmail, and turning on mandatory STARTTLS, SSL or TLS encryption in the settings of your email client. For Gmail, connecting using a recent version of the Chrome or Firefox browser will ensure you have such a secure connection. This practice will help ensure that someone operating on a network between you and your email server cannot read or alter your email in transit. Note that if your email is sent to someone outside of your organization, you cannot control the connections between your email server and the recipients' servers, nor how the recipients access the message—so it is still vulnerable to attack. Because you control your organization and mail server, following this practice may improve the overall security of internal email but is not justification to send sensitive information using email internally or externally.*		★★★	🛠🛠🛠	🗲
5. Where you can, implement two factor authentication for email accounts. *Many email providers have begun to offer login systems that rely on more than one piece of information to identify yourself. There can be several, but usually there are just two: your password and another code you have. Often this is a code sent by text message to your phone but can also be embedded on a special type of USB device, a program that generates codes on your phone, or even a piece of paper with preprinted codes. Users will have to get used to having this extra step to login to new devices, but it protects from someone who obtains either a password or the other item from getting into the account.*		★★★	🛠🛠	🗲🗲🗲

LEGEND ✔ Record actions ★Difficulty rating 🛠 Technical skill level 🗲Work flow disruption

Email Safety Tasks	✔	★	🛠	🗲
6. Don't send email attachments unless you are using encryption. *Unencrypted mail attachments are not protected from being viewed or altered between recipients, and they tend to stay in email boxes, where they are harder to control. Perhaps more important, regular use of attachments builds and encourages a culture of opening them automatically, which is a major source of viruses, malware and associated intrusions. A better practice is to have files on a server and send links to documents instead of the documents themselves. Ideally these links lead to locations that themselves are protected by passwords or other authentication, or are temporary and expire soon after use.*		★★★	🛠🛠🛠	🗲🗲
7. Be very careful clicking links or opening attachments in emails. *Links, often innocuous looking or even hidden within emails, are a major way adversaries get rogue software inside networks. Before clicking a link or anywhere on an email, check that it points to a domain name (such as roadmapconsulting.org) that you recognize and expect (in most email programs, as on the web, hovering over a link displays the URL it points to). If not, check with the sender to make sure you aren't being scammed. Similarly, don't open an attachment unless you are expecting it and the filename is in line with that expectation.* ***NEVER*** *open links or files from unknown senders or in otherwise suspicious emails.*		★★	🛠🛠🛠	🗲🗲
8. Don't send mass email from standard accounts; instead, use a third-party service and if possible a dedicated mass email subdomain. *Sending bulk email from regular email accounts can lead to all sorts of problems for mail delivery, primarily by having your accounts or domain name marked as a source of spam. You may also wish to send bulk email using a separate domain name from your main email (such as comms.roadmapconsulting.org) to further differentiate the traffic and reduce the risk of delivery problems for your regular emails. Additionally, ensuring all email lists are opt-in (people have to confirm they want to receive them) and including instructions on how to discontinue them will minimize the chance of your emails being marked as spam by recipients.*		★★★	🛠🛠🛠	🗲🗲

LEGEND ✔ Record actions ★Difficulty rating 🛠 Technical skill level 🗲Work flow disruption

Email Safety Tasks	✔	★	🛠	🗲
9. Pay for a service to filter spam and viruses from email before it reaches your inbox *This service comes included if you use Gmail, but doesn't with all email services. Filtering mail before it reaches your network lessens the chance of a virus or malware bearing link or attachment being clicked on. After initial setup, this service will be nearly invisible to staff, but requires that someone is tasked with dealing with false positives and other email delivery problems. Be aware, however, that this item involves a significant tradeoff: filtering means that another company is viewing your email before it reaches you and so may increase risk of that information being exposed. The Electric Embers Cooperative (http://electricembers.coop) offers such a service specifically for non-profits.*		★★	🛠🛠🛠	🗲
10. Where email is accessed on mobile or laptop devices, configure email clients and web browser to store as little information as possible. *Most web browsers can and should be set to clear their cache when closed. Most email clients can be configured to not store email offline and to clear caches when closed. Both can be configured not to store passwords as well. By configuring both this way, a lost laptop or phone can result in far less information disclosure. Note that it may also mean that you need to enter a password every time you start the program, and that you cannot access emails without an Internet connection. Thus, this will likely have an extreme operational impact to your team.*		★★	🛠🛠🛠	🗲🗲🗲🗲
11. Establish an email phishing training and education program and test staff through live testing. *"Phishing" is where emails are crafted to look as legitimate as possible in order to get you to click a link or attachment. This is actually a social engineering attack more than a technical one, and so addressing the human element through education is the best way forward. Testing people by sending fake, innocuous phishing emails, is a hard task, but recommended to give people a chance to practice without bad consequences. There are multiple companies that offer this training if you don't have internal capacity to provide it yourself. Contact RoadMap for referrals.*		★★★★	🛠🛠	🗲🗲🗲

LEGEND ✔ Record actions ★Difficulty rating 🛠 Technical skill level 🗲Work flow disruption

Email Safety Tasks	✔	★	🛠	🗲
12. Set up correct DKIM and SPF records for your email domains and subdomains. *These are highly technical steps made in conjunction with your email and Domain Name Service providers to minimize the ability of spammers or phishers to fake emails from your organization. "Hard fail" settings are preferred for SPF records wherever possible. Once set up, this should have minimal impact on day-to-day operations, though it makes changing your email provider or infrastructure more complex. Find more information at http://dkim.org and http://www.openspf.org/.*		★★★★	🛠🛠🛠🛠	🗲
13. Use PGP encryption to secure your email "end to end." *This is a highly technical and labor-intensive initiative to undertake, but probably the most complete way to minimize any inadvertent disclosure of data through email. It will likely require significant changes to staff practices. The most common tools for using PGP encryption with email are the Mozilla Thunderbird email client and the associated Enigmail plugin. You can find a guide for that setup at https://securityinabox.org/en/guide/thunderbird/windows. OSX's Mail program and open source add on GPGTools (https://gpgtools.org) is also a workable tool set for using PGP encrypted email on Macs. Outlook requires a commercial add-on from Symantec to use PGP encryption on Windows. For organizations with more resources, S/MIME is an alternate encryption scheme that works well with a Microsoft Exchange/Outlook environment. If you are interested in either of these solutions, talk to your technical support provider and be prepared to invest some time and resources into planning, implementation and training.*		★★★★	🛠🛠🛠🛠	🗲🗲🗲🗲

Please Note: *Although these practices are highly recommended they do not in and of themselves constitute a successful security practice. Information security is an ongoing process of managing risk and no list of procedures is an adequate replacement for a thorough review of what information you are protecting, why and from whom paired with an organizational commitment to shifting operations to mitigate risk. Information Ecology, RoadMap Consulting and Common Counsel are not liable for negative outcomes associated with following these practices.*

Password and Authentication Safety Checklist

This checklist provides a number or practices that can help you and your staff better curate your organization's passwords and control who accesses your information. While passwords are the most common form of proving your identity to a computer system (aka authentication), other systems are emerging that offer better protection. Some are mentioned below.

In the recommendations below, the term “organizational” is used to identify the group of accounts that grant access to your online identity, backups, administrative controls and other critical systems. These tend to be used infrequently, but are very powerful. As such these passwords should be treated different from “everyday” credentials which is the set of passwords members of the staff needs to perform their regular duties – for things like databases and communication tools.

LEGEND ✔ Record actions ★ Difficulty rating 🛠 Technical skill level 🗲 Work flow disruption

Password and Authentication Safety Tasks	✔	★	🛠	🗲
1. Use strong passwords for all accounts, organizational and everyday. *Strong passwords are generally longer than 8 characters, use a mix of symbols, numbers and both upper and lowercase letters, and do not include any dictionary words or personal information. There are many ways to generate strong passwords. There is an online guide to creating passwords as part of the excellent Security In a Box website you can find here: https://securityinabox.org/en/guide/passwords. Diceware is another excellent method for creating good passwords: http://world.std.com/~reinhold/diceware.html. Most password managers will make a random password for you, as will other available software for that specific purpose.*		★	🛠	🗲
2. Don't use the same password for more than one site or service. *If you don’t reuse passwords, someone learning your username and password for one service won't get easy to access the other accounts you use. Use different passwords so you aren’t relying on the provider to protect your most important secret.*		★	🛠	🗲🗲
3. Try to limit written password storage. *Instead use techniques found in the Security In a Box online guide listed above to create memorable but strong passwords. If you initially need a written copy of your password, protect it physically by storing it someplace like your wallet. Try to type your password with less looking at the copy each time, and destroy the paper copy when you have memorized the password. If you are having trouble memorizing passwords, use a password manager as indicated in #5 below.*		★	🛠	🗲
4. Do not tell anyone else your password(s), ever. *Even if someone claims to be from IT or technical support, do not*		★	🛠	🗲

LEGEND ✔ Record actions ★Difficulty rating 🛠 Technical skill level 🗲Work flow disruption

Password and Authentication Safety Tasks	✔	★	🛠	🗲
give them your password. Nearly every system allows for administrative reset of passwords for maintenance. This creates an auditable trail that your account was accessed and alerts you as well. Although changing your password afterwards is an extra step, it will ensure that you and only you have access to your digital information.				
5. Have all staff use password manager software. *There are many passwords associated with modern work flows, and they need to be protected. They shouldn't be stored in spreadsheets, text files or word processor documents (even password-protected ones as they are simple to break open).* *Instead, password manager software is available, which stores all of your passwords in a secure file and can easily take care of all of the checklist items above. To use password manager software, you just remember a single password to open your secure file of passwords. This makes it much easier to then can have an array of unique, complex passwords for all your services.* *Password managers are available as software that you install (e.g., KeePass) and as a web-based service (e.g., LastPass). KeePass and KeePassX use the same encrypted file format, can run on almost any computer, and so are recommended password managers. Security In a Box also has a KeePass overview here: https://securityinabox.org/en/guide/keepass/windows.* *The central role of web-based accounts in many organizations has made web-based tools for password management very popular. However, web browsers are insecure environments for password storage and handling. Evaluating online services and their current security claims is outside of the scope of this document. We acknowledge that online password management tools often have adequate security levels for many organizations' everyday password handling needs; however, they are not recommended for storing core organizational passwords or other highly sensitive information.*		★★	🛠🛠	🗲🗲🗲
6. Separate organizational and everyday passwords. *Organizational passwords include any passwords that grant administrative control of your organization's information systems or online identity. These are very powerful credentials and so should be stored separately from passwords that just get staff into their personal user accounts. You can do this by making a separate login or file in your password manager application, or by choosing a completely different manager altogether.*		★★★	🛠🛠	🗲🗲🗲

LEGEND ✔ Record actions ★Difficulty rating 🛠 Technical skill level 🗲Work flow disruption

Password and Authentication Safety Tasks	✔	★	🛠	🗲
Placing organizational passwords in a KeePass file that only a few key staff members can access will lessen the risks of adopting an online password manager for everyday passwords, but will also place a burden on those staff members. Balancing these needs should be factored in your decision.				
7. Use two factor authentication wherever possible *Many companies have begun to offer login systems that rely on more than one piece of information to identify yourself. There can be several, but usually there are just two: your password and another code you have. Often this is a code sent by text message to your phone but can also be embedded on a special type of USB device, a program that generates codes on your phone, or even a piece of paper with preprinted codes. Users will have to get used to having this extra step to login to new devices, but it protects from someone who obtains either a password or the other item from getting into the account.*		★★★	🛠	🗲🗲🗲
8. Consider making single use passwords for sites you rarely use. *If you need to create an account for something that you do not expect to use frequently and where you can reset the password easily by email, you may just wish to generate a very long random string of numbers, letters and symbols and not record it anywhere or remember it. Most password managers will make a random password for you, as will other available software for that specific purpose. This service will now have a password stronger than if you made one and tried to remember it.* *The next time you need to login to that service you can hit the "forgot password link" to get a login link and repeat the process. This is a little slower, perhaps, than a stored password but the benefit is that you will never leak your password for that tool – because you don't know it! Of course you wouldn't do this with an account you use all the time but it is useful to ease the password management load. Recognize that this reduces the security of the account using a "single use" password to the security of your email account (since you use that to get back into the service), so your email password needs to be strong and memorable.*		★★★	🛠🛠	🗲🗲
9. Set minimum password lengths and enforce complexity rules on services where you can do so, and regularly monitor user password strength. *On many platforms including Windows Active Directory and Google Apps you can set controls at an administrative level to ensure people use strong passwords. It takes some advance planning and*		★★★★	🛠🛠🛠🛠	🗲🗲🗲

LEGEND ✔ Record actions ★Difficulty rating 🛠 Technical skill level 🗲Work flow disruption

Password and Authentication Safety Tasks	✔	★	🛠	🗲
staff training, as setting up these controls without being clear on the implications can lock people out of their computers or work files. In addition, someone will need to be designated as the point person for resolving problems that arise from these controls. This step does, however, improve the security of all users at one time so is highly recommended.				

Please Note: *Although these practices are highly recommended they do not in and of themselves constitute a successful security practice. Information security is an ongoing process of managing risk and no list of procedures is an adequate replacement for a thorough review of what information you are protecting, why and from whom paired with an organizational commitment to shifting operations to mitigate risk. Information Ecology, RoadMap Consulting and Common Counsel are not liable for negative outcomes associated with following these practices.*

Public Wireless Network Safety Checklist

This checklist provides a number of practices that can help protect you and your staff when using publicly available wireless networks such as those in hotels, cafés and airports. Because there are so many ways that wireless networks can be compromised, this checklist is not exhaustive.

If performing work using sensitive or confidential information, including that required to be protected by law (such as personal health information, employment records and credit card numbers), you are best off avoiding the use of public networks for those tasks.

LEGEND ✔ Record actions ★ Difficulty rating 🛠 Technical skill level 🗲 Work flow disruption

Public Wireless Network Safety Tasks	✔	★	🛠	🗲
1. Keep all web browser software, including extensions, updated to the latest version. Prefer Firefox or Chrome browsers. Only use Internet Explorer and Safari when required. *Internet Explorer has had a much higher incidence of vulnerabilities than Chrome and Firefox, while Safari has suffered some recent security concerns. Although nearly all of the latest browsers support "certificate pinning," which makes it harder to intercept secure connections, Chrome and Firefox have led the development of this important feature. These browsers can be downloaded from https://getfirefox.com and https://google.com/chrome.*		★	🛠	🗲
2. Install the HTTPS Everywhere extension for all of the web browsers you use on your system. *This step will help ensure that more sites you visit and information you submit to them cannot be seen by others on the wireless network or the operator of the network itself. You can install the extension from the following page: https://www.eff.org/HTTPS-EVERYWHERE.*		★	🛠	🗲
3. Install Privacy Badger, a browser add-on which will limit the "cookies"—small persistent chunks of information—set on your computer by websites. *Privacy Badger is software produced by the non-profit Electronic Frontier Foundation (https://eff.org) to help reduce the privacy breaches and tracking that come with the use of cookies. These cookies can be transferred insecurely so can, if poorly implemented, expose login credentials or other information in transit. As an extra benefit, you will increase your privacy and lessen your online tracking as a result of using this software. Download it at https://privacybadger.org.*		★	🛠	🗲

LEGEND ✔ Record actions ★Difficulty rating 🛠 Technical skill level 🗲Work flow disruption

Public Wireless Network Safety Tasks	✔	★	🛠	🗲
4. Confirm the network details before you connect. *An attacker can setup an access point with a name similar or identical to a legitimate one, so that you connect to it instead of the network you intend. Make sure to ask the proprietor of a public network what the network name and password are, and connect to the network with that name that accepts that password. This doesn't completely guarantee that the network you are connecting to isn't hostile or compromised, but it makes the difficulty of hijacking your connection much higher.*		★★	🛠	🗲
5. Turn off the built-in file sharing functionality on your computer or device. *Although handy for sharing files with peers, the built-in file sharing functionality on your computer is vulnerable to abuse or accidental information leakage. It is preferable to set up alternate tools and practices for sharing files, such as a central file repository.* *To turn off file sharing on a Mac, go to Apple menu > System Preferences, then click Sharing and make sure all the boxes are unchecked.* *See this article for turning off file sharing on a Windows computer: https://support.microsoft.com/en-us/kb/307874.* *Recognize that if you are currently using the built-in file sharing functionality to share files inside an office, doing this will disrupt current work practices.*		★	🛠	🗲🗲
6. Turn on your computer's firewall and disallow all external connections. *A firewall prevents unauthorized connections from other computers on the wireless network. There is a built-in firewall in every computer, but it is not turned on by default and may allow connections to certain services. The firewall settings can be found on Macs in System Preferences>Security. On Windows computers, the firewall settings are in the System and Security tool in Control Panel. More information about Windows Firewall can be found here: http://www.microsoft.com/security/pc-security/firewalls-using.aspx.*		★★	🛠🛠	🗲🗲

LEGEND ✔ Record actions ★Difficulty rating 🛠 Technical skill level 🗲Work flow disruption

Public Wireless Network Safety Tasks	✔	★	🛠	🗲
7. Ensure that the wireless network is not presenting false certificates *Increasingly networks are setup to monitor traffic for various reasons such as ad placement or content filtering. The way they do this is called a Man-In-The-Middle (MITM) attack. The network device will replace the security certificate from the service that you are connecting to with one of its own. Anyone with access to that device can see any communication between you and that service. Learning to view certificates in your web browser, or installing and learning to use a tool such as Certificate Patrol (available only for Firefox; read more at http://patrol.psyced.org/) will help you identify false certificates.* *Viewing certificate information in Chrome:* *https://support.google.com/chrome/answer/95617?hl=en* *Viewing certificate information in Firefox:* *https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure* *https://support.mozilla.org/en-US/kb/secure-website-certificate*		★★★★	🛠🛠🛠	🗲🗲🗲

LEGEND ✔ Record actions ★Difficulty rating 🛠 Technical skill level 🗲Work flow disruption

Public Wireless Network Safety Tasks	✔	★	🛠	🗲
8. Use a Virtual Private Network (VPN) to securely tunnel out of public networks. *A VPN creates a secure connection for your computers to use to access the office network and the Internet. This connection, or tunnel, can be used to hide all information moving from your computers to the Internet or office network from the operator or other users of the wireless network. Use of a VPN severely limits the amount of trust you have to place in the owner and operator of the network you are on and so limits your exposure to them. These factors make VPNs a very effective way to protect yourself on untrusted networks.* *A VPN is implemented via a device you own located in your office or at an offsite facility, or that a third party provides you use of for a fee. Choosing a VPN provider and setting up computers to use it are not simple tasks, and critically important—a misstep in setup or use can expose your information or slow your work to a crawl. In addition, VPNs add a layer of network traffic and will slow down your Internet access, so your distance to and bandwidth available from your VPN provider (or your office if hosting your own) will make a difference to performance.* *Consider if the speed tradeoff is acceptable to you before choosing to implement a VPN. If you do, the investment in implementation, setup, and hassle is repaid by a solution that significantly increases your security while using untrusted networks.*		★★★★	🛠🛠🛠🛠	🗲🗲🗲

Please Note: *Although these practices are highly recommended they do not in and of themselves constitute a successful security practice. Information security is an ongoing process of managing risk and no list of procedures is an adequate replacement for a thorough review of what information you are protecting, why and from whom paired with an organizational commitment to shifting operations to mitigate risk. Information Ecology, RoadMap Consulting and Common Counsel are not liable for negative outcomes associated with following these practices.*

Constitutional Communications Strategic Security Planning

I. Frameworks for security:

There are four basic frameworks that CC uses in our security assessment and analysis process.

- First, security is a process, not an event. A secure process manages and minimizes risk. Risk can be defined as "a future uncertain event" and is measured in terms of likelihood and impact. No amount of security measures can ever totally eliminate risk. Over protection leads to a waste of resources and under protection leads to an unwarranted risk. Security measures selected must be balanced and cost effective in their application.
- Second, we use a team "network" effect in order achieve much more rapid deployment of communications technology.
- Third, because of the development of free and open source computing and encryption technology, high degrees of digital security are accessible and cost effective, even to under resourced non-profit organizations.
- Forth, the adoption of new tools will only prove effective if they are applied in the current workflow of an organization. The adoption and security strategy must be tailored specifically to the needs of the people doing the daily work of the organization, with knowledge and training about how important their diligence and security is to the group as a whole.

  The specifics of CC's digital security concept revolve around organizational reputation, individual integrity, free and open-source software transparency, and encrypted data/communication channels. This puts a high premium on personal competence, collective communication, ethical discipline, and the best possible open source encryption systems. This can ensure that even network penetration or loss of data will not mean the exposure of sensitive information.

  These security perspectives, protocols and tools will collectively maintain attorney and activists' information security and protection of assets from compromise. Compromise is defined as a breach of:
  a) Confidentiality and Security: The restriction of information and other valuable assets to membership (e.g. protection from eavesdropping, and computer hacking).

  b) Integrity: The maintenance of information systems of all kinds and physical assets in their complete and usable form (e.g. protection from viruses on a computer program).
  c) Availability: The permitting of continuous or timely access to information systems or physical assets by members (e.g. protection from sabotage, malicious damage, theft, fire and flood).

II. Information Security Categories: ConComms uses three secure communication categories to help groups organize their information on the basis of threat actors, risk and impact of breach:

1. **Public, Internal, and Confidential.**

a) Public is defined as information that is designed to reach a specific platform or party, which poses no harm and is designed to be released to a wide audience. (i.e. Twitter posts, general lunch invitations).

b) Internal is information that should be kept from the public, which some threat actors may want to expose and which could undermine trust in CCR if exposed (i.e. Unencrypted emails about general problems with other groups). While we need to protect Internal information from adversaries like right wing hackers, we expect Internal information will have its metadata and content collected and analyzed by the US government or other large threat actors.

c) Confidential is information that could put activists, clients or staff at risk if aggressive threat actors accessed it. It may involve strategic planning; attorney client privileged information, personnel names and addresses, or relationships with highly threatened groups who are under significant risk. Confidential information is always encrypted in an open source system, either end-to-end encryption in transit, or symmetric encryption at rest. Confidential information may also obscure metadata as well as content. This means no adversary will be able to see what protected parties are saying, or who is communicating with whom.

We will use these categories to organize different aspects of organizations information, assess the workflow needs and threat analysis with key staff. Once information is broken up into these three categories, each corresponds to a different level of necessary protection, correlating to the maximum likely threat posed by its exposure, be it in the form of hackers with no special access, mass/passive collection (by governments and private service providers), or targeted (active) surveillance via network penetration (sniffing or back doors) and endpoint penetration. The goal is to ensure that Public information is accessible but all Internal, and Confidential communications and information is appropriately protected even from the highest levels of penetration. The Confidential channel can be used for some leadership functions and inter-organizational relationships to effectively obscure confidential communications. When properly implemented, this channel can fully eliminate or effectively obscure all content and metadata, including names, geolocations, IP addresses, ISPs, and other markers in order to uphold trust and security for organizers facing active threats.

A) Strategic security planning: What threats from which adversaries pose the highest risks to your assets?

✓ Threat: What you are protecting against?
A brief description of the type of threat/attack
✓ Potential Impacts: What you are protecting against?
A brief description of the impact of such a threat/attack
✓ Adversaries: Who is posing the threat?
A brief description of the adversary (known, unknown; government, non-governmental; associations)
✓ Assets Affected/Involved: What you are protecting?
A brief description of the assets, resources, people affected
✓ Protections in Place: A brief description of what you already have in place to protect against the threat?

What capacity can you develop to make that protection more robust?
✓ Risk: Likelihood of the threat occurring? For your organization, indicate here what are the criteria that makes the likelihood of a threat high, medium (med), or low?

High –
Med –
Low -

✓ Impact: If the threat is realized, what is the impact on the organization? For your organization indicate, here what are the criteria that makes the impact high, medium (med), or low?

High –
Med –
Low -

✓ Compartmentalize; take the most time on securing info where the risk is highest, and asset is most important to your work.

B) How to begin the compartmentalization process:

1) First make a group decision on what type of information are your organizations most significant secure assets.
2) Then focus where the likelihood and the impact are greatest to those assets
(Examples: Passwords, crisis response, action planning, strategic planning, HR and Personal Identifiable Information (PII), Social Security numbers, bank details, member database)
3) Then triage current organizational systems with capacity and security needs.
4) Ask the question: What capacity can we add to the most critical information asset, with the least effort and best long term impact?
5) Only build in new capacity tools when it is clear that Signal, Tor, Onionshare, etc. can't do the job; because of usability or information type.

C) What are "assets" in your organizing?
Things that may be assets in your work (different for each context and organization):

1) Organizational staff information, member information, target population data (criminal convictions, HIV status, immigration status, LGBTI status) Health or addiction info (contextual)

2) Donor relationship and strategy, donor lists, foundation relationships.

3) Any combination of Personally Identifiable Information and HR information that could be combined to create Identity Theft. (Full name, Social Security #, birth date, address, email, phone, and all photos of ID's, passports and state licenses of staff and others)

4) Relationship and strategic planning with targeted groups Internationally or within the US. This may require the capacity to protect communications metadata with targeted groups, this may include, key organizers or leadership in strategic campaigns, politically targeted groups like whistle blowers, immigrants, POC, ideological adversaries of powerful parties like communists, radicals, socialists, dissidents or anarchists. (Context and temporally specific).

5) For many journalists or publishing organizations this may involve: Source names, communications and contacts, correspondence with the editor, time sensitive research, drafts of documents and articles, and collaborators.

6) For many legal organizations that may involve financial information of donors and employees, contacts lists of partners and clients, client statements, affidavits, advocacy strategies.

7) Banking information: Including account numbers, routing numbers, security questions, passwords, pins and contact info attached to the account.

8) All organizational credentials (login, password, user name etc.), or personal accounts used for organizational work. All credentials for recovery accounts or other backup accounts.

D) Get a picture of what information systems your organization is currently using for work:

Contacts Database:
1) Do you have Contacts management/database?
2) Is there a formal CRM that you are using?
3) What are the other ways you keep contact information? Spreadsheets? Email?
4) Are your contacts syncing across devices? Which service is used for syncing?
5) Do you have a self-hosted database Server? Or is the data stored with a third party?
6) What are all the databases you have in use?
7) What kinds of contacts or what types of contact data might be sensitive?
8) Do you have a system to keep sensitive/confidential contact info secure?
9) Do they have non-public information stored on the backend of your website?

File sharing:
1) Describe the ways you know that people pass documents or files to one another.
2) Do you host a file server that is used day to day for filesharing? How is that server configured and where is it stored?
3) Are some people failing to use that system?
4) Are email attachments in use? Are they shared within the organizational system?
5) Thumb drives in use for document sharing?
6) Do you use third party services like Google or Dropbox for document sharing? Are staff given organizational accounts, or do they use personal accounts for such document sharing?
7) How is email used for communications?
8) What email system is in use?

Password and account credentials:
1) Where are the passwords for e-mail, social media, and cloud services accounts saved? Who has access to them? Are unique passwords used for each account? Have they ever been shared in an unencrypted manner? How?
2) Do you have a password manager? How is it maintained?
3) How do you share passphrases from one staffer to the next?
4) Do you keep track of who has what passwords?
5) Do passwords for organizational accounts get updated?
6) Do you enforce passphrase length and complexity on all staff?
7) Do you enforce uniqueness requirements on all staff?
8) Does someone have access to all the credentials for accounts set up by individuals in the organizations name?
9) Do you have a system for privileged or confidential communications? What is that system? Where is data stored? How is it backed up? How is it encrypted?
10) Is your organization currently using staff encryption keys? How are the private keys managed and maintained?

11) What are the recovery options for your accounts? How are the recovery accounts secured?

Backups

1) Do you have a regular process of backing up key information systems? What systems are backed up? How often?
2) Where are they back up to? How are the backup secured?
3) Are shared files backed up? How?
4) Is your server or CRM backed up? How?
5) Are Individual laptops/workstations backed up? How?

Grant applications

1) Tell us the story of contact points between grant application and follow up?
2) How are grants applied for? How are applicants contacted?
3) How are funders communicated with during and after the project period?

Legal actions:

1) Is the organization involved in any legal actions that require security for witnesses or 3rd parties? How is that information secured?
2) Is leadership directly involved in security management? Is there another organizational role whose responsibility it is?
3) Where are passports/personal ID documents maintained in the organization? Are they accepted in an encrypted way and stored in an encrypted database/file?
4) Do you often book flights for staff? How do you manage their flight and personal information?
5) Where do you pay taxes? Who handles your tax information? How is it secured prior to submission?
6) Are you involved in compiling or maintaining evidence, witnesses, and contact info of (metadata) specific source personal information for human rights reports?
7) Are you involved in compiling or maintaining witnesses, metadata and personal information on sources for investigative journalism work?
8) Is your organization ever involved with or maintaining bank statements, checking accounts or wire transfers to targeted groups, especially in other countries?
9) Are you involved with support for targeted groups (immigrants, dissidents, Etc.), how do you secure the metadata, identities and whereabouts of those individuals?

Internal Strategic Planning:

1) How are board reports compiled? Where are board reports saved? Are there non-public aspects to a board report?
2) Where are your internal strategy and assessment documents saved? How to you share and maintain organizational strategy documents?
3) How to you share and maintain organizational strategy documents from partners?
4) Where are internal employee assessments, employee health and banking information saved?
5) Are you involved in legal actions where you maintain trial strategies, and legal negotiation positions? How are these secured and shared?

Structural hardware and network concerns:

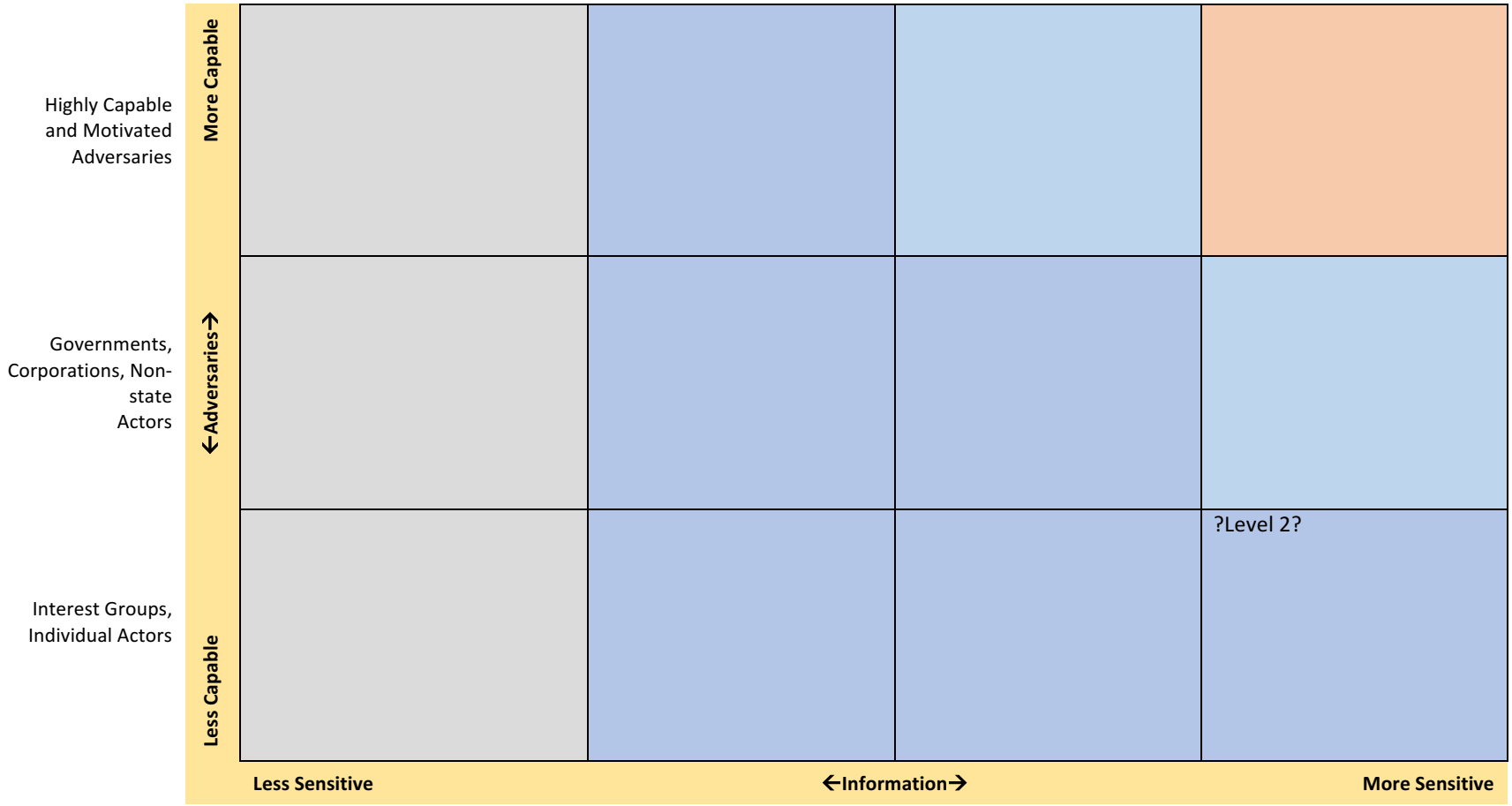
1) Does your staff ever use “Open Wi-Fi” access from work related computers?
2) Do you allow for Wi-Fi access to your office server?
3) How often are work devices purchased and updated?
4) Is device geolocation data of cell phones of computers in proximity to targeted individuals an organizational concern?

E) Finally, implement new capacities for high risk confidential assets, using the Threat Matrix.

Threat	Potential Impacts	Adversaries	Assets Affected/Involved	Protections in Place	Risk	IMPACT
	•	•	•			
	•	•	•			
	•	•	•			
	•	•	•			
	•	•	•			

Compartmentalization Strategy
Compartment: Types of information: Technical requirement:
Compartment: Types of information: Technical requirement:
Compartment: Types of information: Technical requirement:
Compartment: Types of information: Technical requirement:

(1) Map your information, and Adjust your work flow accordingly.
(2) Workflow Security Level:
Level 1 (Confidential/targeted), Level 2(Confidential), Level 3 (internal), Level 4 (public)



Changes in Workflow, in additional to basic security practices

Required
• Signal message encryption
• Full disk and device encryption
• Only use organization-issued computer and phone (if part of a larger organization)
	Required
	• End-to-end encryption for all communications
	  ○ Email with PGP/GPG
	  ○ End-to-end encrypted messaging and voice with Signal
	  ○ Document sharing with Onionshare
	  ○ Meeting with Jitsi Meet
	• Border crossing security
		Required
		• Consultation with trusted security agents

Recommended • End-to-end encryption for all communications • Border crossing security	**Recommended** • Consultation with trusted security agents	**Possibilities** • Only work on computers disconnected from the internet • No communications that are not end-to-end encrypted • No closed systems for communications ○ No Skype, Whatsapp, telegram, etc.

Example Threat Matrix:

PLEASE CUSTOMIZE FOR YOUR ORGANIZATION

Threat	Potential Impacts	Adversaries (be specific as possible)	Assets Affected/ Involved (be specific)	Protections in Place (be specific)	Risk / Likelihood	IMPACT LEVEL
Example: Physical attack	• Staff may be injured, killed, kidnapped, traumatized • Non-injured staff traumatized • Operations stop • Time spent providing staff and community support	• Anti-X stranger • Police/law enforcement who believe we are enemies of the state • Groups/Individuals against occupants in our building (e.g., Planned Parenthood)	• Staff • Office space and surrounding area • Physical files and computers	• High security building • Secure communications process in place for crisis	**LOW**	**HIGH**
Example: Schmear campaign against org	• Funders lose trust in organization • Allied orgs lose trust in organization • Research considered suspect • Time spent communicating with constituents to regain trust	• Anti-X opposition • Elected officials supported by anti-X opposition	• Org reputation • Staff reputation • Funder reputation • Ally org reputation	• High security building • Secure communications process in place for crisis	**MED**	**HIGH**

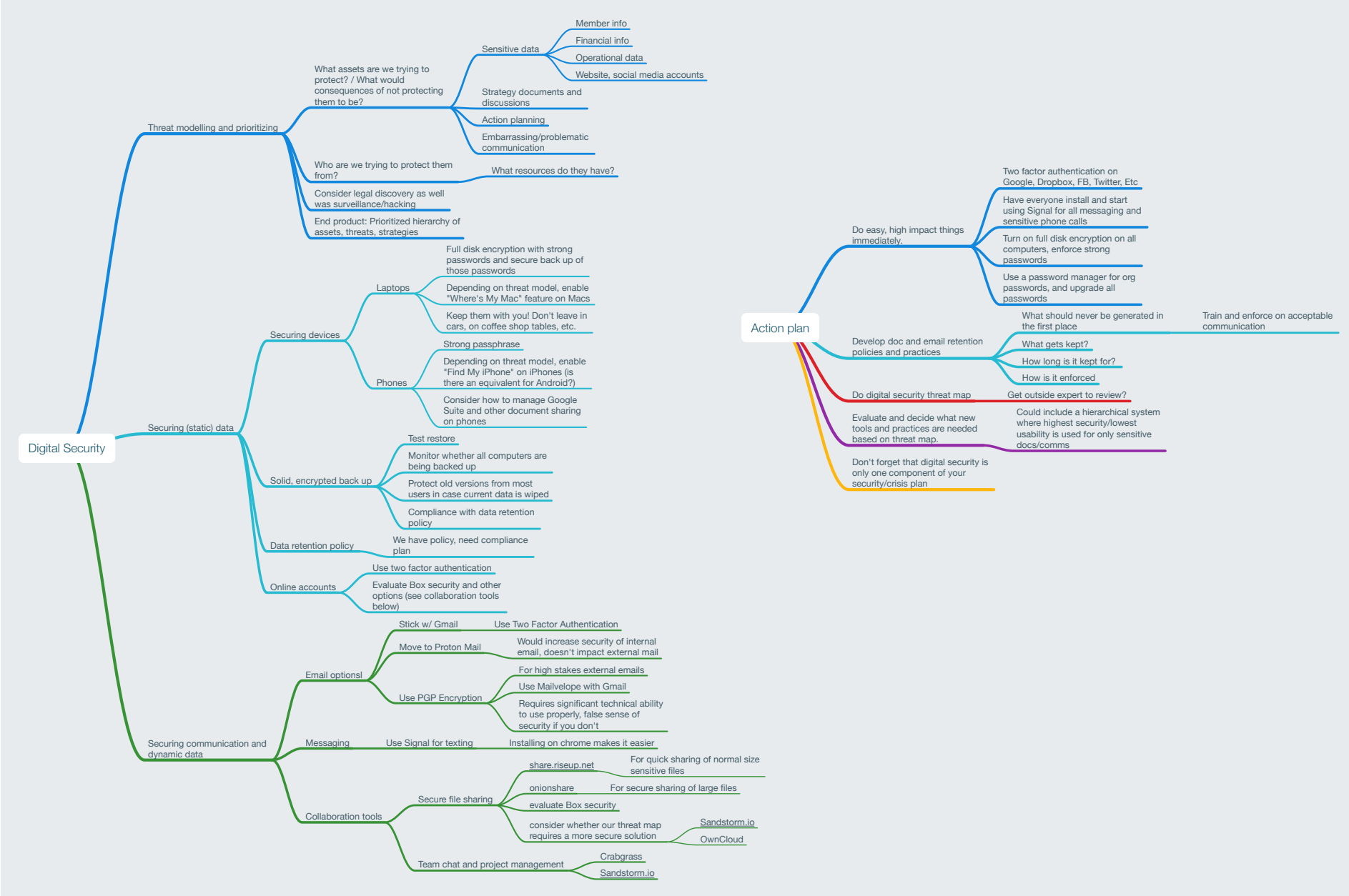
Threat	Potential Impacts	Adversaries (be specific as possible)	Assets Affected/ Involved (be specific)	Protections in Place (be specific)	Risk / Likelihood	IMPACT LEVEL
Example: *Email hacked*	• Emails sent in the name of organization • Personal information about staff are disclosed, leading to staff safety issues • Organization and staff are targeted with schmear campaigns • Email exchanges between org staff or to external parties are taken out of context • Time spent communicating with constituents to regain trust	• Anti-X opposition • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring)	• Email server • Emails of individuals • Contact information stored through email client	• High security building • Secure communications process in place for crisis	**HIGH**	**HIGH**
Example: *Bank assets frozen*	• Unable to access money to pay staff and other expenses • Organization and staff are targeted with schmear campaigns • Time spent investigating, recovering, resetting, and re-securing account • Time spent communicating with donors	• Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring) • Bank administration?	• Money	• Assets distributed across different banks • Cash on hand • Conversations with funders to enable access of emergency funds	**MED**	**HIGH**

Threat	Potential Impacts	Adversaries (be specific as possible)	Assets Affected/ Involved (be specific)	Protections in Place (be specific)	Risk / Likelihood	IMPACT LEVEL
Example: *Financial theft / unauthorized*	• Money is stolen • Unauthorized charges • Time lost investigating, recovering, resetting, and re-securing accounts • Time spent communicating with donors	• Anti-X opposition infiltrator •	• Money	• Assets distributed across different banks • Cash on hand • Conversations with funders to enable access of emergency funds	**LOW**	**MED**
Example: *Database (DB) hacked*	• Individuals in DB are targeted physically • Individuals in DB are targeted for arrest, electronic surveillance, or deportation • Time spent investigating, recovering, resetting, and re-securing account; time lost communicating with affected contacts	• Anti-X opposition • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring)	• Contact information of clients, constituents, and collaborators	• Password protected • Segmented access to DB information (on a need-to-know basis) • Individuals in DB are not conducting activities that might be targeted by	**HIGH**	
Example: *Social media hacked*	• Messages sent in the name of organization • Organization and staff are targeted with schmear campaigns • Time spent investigating, recovering, resetting, and re-securing account; time lost communicating with constituents to regain trust	• Anti-X opposition • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring)	• Facebook • Twitter • …	• Only those who need access have access • No automatic sign-ins from browser; no passwords save on browser		

Threat	Potential Impacts	Adversaries (be specific as possible)	Assets Affected/ Involved (be specific)	Protections in Place (be specific)	Risk / Likelihood	IMPACT LEVEL
Example: *Shared document repository*	• Unable to access key documents • Account and passwords compromised • Time spent investigating, recovering, resetting, and re-securing documents • Time spent communicating to anyone who had access to documents that were compromised	• Anti-X opposition • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring)	• Online storage (e.g., Dropbox, Box, Google Drive/Apps, Sharepoint) • Documents	• All generic permissions have been removed; • All documents are shared with specific people only • No automatic sign-ins from browser; no passwords save on browser Backups made nightly? • Access to document and folder is removed once project has been completed • Approved Document Retention and Destruction policy and in practice		

Threat	Potential Impacts	Adversaries (be specific as possible)	Assets Affected/ Involved (be specific)	Protections in Place (be specific)	Risk / Likelihood	IMPACT LEVEL
Example: *Devices stolen or confiscated*	• Cost of lost device • Compromise of sensitive information • Key documents not stored online no longer accessible • Account and passwords compromised, must remember and change all accounts and passwords • Unattended device that is logged-in is stolen and information on that device is compromised • Notifications sent are compromised even on a locked device • Time spent reporting, investigating, and replacing stolen device	• Anti-X opposition • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring)	• Computers • Contact information stored locally • Phone call records, instant/chat messages • Works in progress	• Computers password protected • Password protected screensaver every X minutes • All devices are password-protected / locked • Find my device / Locate stolen device / Find Friends activated (staff know how to turn off if they need to be 'not found')		

Compartmentalization Strategy
Compartment: PUBLIC Types of information: Public information, press releases, tweets Technical requirement: Twitter account, Facebook account, etc.
Compartment: DONORS Types of information: Donor contact information, non-publically available information Technical requirement:
Compartment: INTERNAL Types of information: Organizing strategy Technical requirement: Email, Signal, Jitsi.org
Compartment: STAFF Types of information: Personnel information Technical requirement:
Compartment: SECURITY Types of information: Crisis communications, passwords and social security numbers Technical requirement: Onionshare and signal
Compartment: TEXT/CHAT/SMS MESSAGING Types of information: emergency/private communications Technical requirement:
Compartment: Types of information: Technical requirement:


Digital Security
Threat modelling and prioritizing
What assets are we trying to protect? / What would consequences of not protecting them to be?
Sensitive data
Member info
Financial info
Operational data
Website, social media accounts
Strategy documents and discussions
Action planning
Embarrassing/problematic communication
Who are we trying to protect them from?
What resources do they have?
Consider legal discovery as well was surveillance/hacking
End product: Prioritized hierarchy of assets, threats, strategies
Securing (static) data
Securing devices
Laptops
Full disk encryption with strong passwords and secure back up of those passwords
Depending on threat model, enable "Where's My Mac" feature on Macs
Keep them with you! Don't leave in cars, on coffee shop tables, etc.
Phones
Strong passphrase
Depending on threat model, enable "Find My iPhone" on iPhones (is there an equivalent for Android?)
Consider how to manage Google Suite and other document sharing on phones
Solid, encrypted back up
Test restore
Monitor whether all computers are being backed up
Protect old versions from most users in case current data is wiped
Compliance with data retention policy
Data retention policy
We have policy, need compliance plan
Online accounts
Use two factor authentication
Evaluate Box security and other options (see collaboration tools below)
Securing communication and dynamic data
Email options!
Stick w/ Gmail
Use Two Factor Authentication
Move to Proton Mail
Would increase security of internal email, doesn't impact external mail
Use PGP Encryption
For high stakes external emails
Use Mailvelope with Gmail
Requires significant technical ability to use properly, false sense of security if you don't
Messaging
Use Signal for texting
Installing on chrome makes it easier
Collaboration tools
Secure file sharing
share.riseup.net
For quick sharing of normal size sensitive files
onionshare
For secure sharing of large files
evaluate Box security
consider whether our threat map requires a more secure solution
Sandstorm.io
OwnCloud
Team chat and project management
Crabgrass
Sandstorm.io
Action plan
Do easy, high impact things immediately.
Two factor authentication on Google, Dropbox, FB, Twitter, Etc
Have everyone install and start using Signal for all messaging and sensitive phone calls
Turn on full disk encryption on all computers, enforce strong passwords
Use a password manager for org passwords, and upgrade all passwords
Develop doc and email retention policies and practices
What should never be generated in the first place
Train and enforce on acceptable communication
What gets kept?
How long is it kept for?
How is it enforced
Do digital security threat map
Get outside expert to review?
Evaluate and decide what new tools and practices are needed based on threat map.
Could include a hierarchical system where highest security/lowest usability is used for only sensitive docs/comms
Don't forget that digital security is only one component of your security/crisis plan

Glossary

Backup. Regularly updated copies of your digital assets, ideally stored in several different places, so that if access to or integrity of your data is disrupted for any reason (damage to computers due to accident or natural disaster, accidental or malicious deletion of files, etc.), the assets can be restored. Online backup services such as Mozy and CrashPlan are best supplemented by backups stored on organizational equipment and in secure offsite storage.

Cookies. Small files placed on your computer by websites that you visit; they are used to manage website features such as logins and can also be used to track behavior on the web. While not all cookies are a security risk, if poorly implemented they can expose the information they contain. More information about cookies is available at http://www.allaboutcookies.org/.

Digital assets. Any and all data electronically stored or used by your organization. This includes your organization's files, website, emails, social media accounts, online banking accounts, etc. Some of these items may be ones that you administer yourself (e.g., the contents of staff hard drives, file repositories stored on servers owned and controlled by your organization); others may be maintained by third-party services on your behalf (e.g., files on Google Drive or Box). Others are services that you participate in that are owned and controlled by others (subject to terms of service), such as organizational Facebook pages.

DKIM records. DomainKeys Identified Mail (DKIM) is a system to protect email from abuse, both from forged sender addresses and from content alteration. The system operates at the server level so requires help from your email provider to setup.

Domain Name System. The domain name system (DNS) is like a phone book for the Internet. It translates domain names (such as roadmapconsulting.org or whitehouse.gov) into the numbers (IP addresses) used to find services on the Internet. It can also be used to store other information about your organization's information systems, such as SPF records or DKIM keys.

Encryption. A mechanism by which your data scrambled in order to protect it from being read by unauthorized parties. Authorized parties are able to decrypt (i.e., unscramble) it. There are many different ways to encrypt communications and other digital assets.

Encryption key. A piece of information that you share with an authorized party so they can encrypt and/or decrypt information to or from you. In many cases this information is highly sensitive and needs to be protected; however, modern encryption methods allow you to have a “public” key that you can safely share with anyone.

Extensions. Small pieces of software that you install as part of your web browser in order to give your browser additional capabilities.

Firewall. A piece of software or hardware device that analyzes and selectively blocks or alters information passing between two networks. Common places to find firewalls are between your office network and the Internet and on your computer to protect you from other computers on your office network.

Office network. The equipment in your office that allows staff computers to connect to each other and to on-site resources such as file servers and to the Internet. If you cannot trust that nobody else is controlling this network, your security progress will be compromised.

Password manager software. Software that keeps your passwords in an encrypted format, protected by a master password. This allows you to store multiple passwords by remembering only one. Password managers are available as software that you install (e.g., KeePass) and as a web-based service (e.g., LastPass). While web-based password managers can be secure enough to hold the passwords staff use to access their accounts for everyday purposes, they are not recommended to store the passwords that grant administrative access to core organizational accounts.

Security certificate. A specific kind of file that includes an encryption key, and often times additional information about that key. Websites such as those used for banking and other services involving sensitive information frequently use them to allow you to establish a secure connection with their servers.

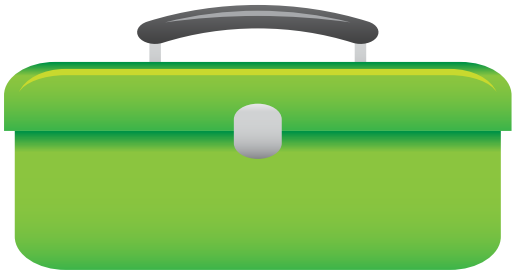
SPF records. Sender Policy Framework (SPF) is a system that allows you to tell others what servers and services are allowed to send email for your organization's domain name. Setting up this record requires the assistance of your DNS provider and can have unintended negative consequences for your email delivery if not properly done.

Virtual Private Network (VPN). A connection between computers that them to exchange information in an encrypted form. This can allow you to both “tunnel out of” a network you don't trust or to get you access to information on your office network from someplace else on the Internet.

Wireless Access Point (WAP). A piece of hardware configured to host a wireless network. In many small networks the WAP will also be a firewall separating the network from the rest of the Internet.

WEP, WPA and WPA2. All are methods of encrypting wireless network traffic between a device like a computer or phone and a wireless access point. WEP is an older encryption method and it is far less secure than WPA and WPA2, which are newer methods.

Section 5: Various Memos, Tools and Documents



Your **TOOLKIT** items in this section include:

5.1 *Understanding and Beating Back Opposition Attacks*
5.2 *Progressive Victory Scale of Organization Data Health*
5.3 *C3 C4 Affiliated Organizations Transactions Flow Chart*

Understanding and Beating Back Opposition Attacks Memo

Opposition attacks on social change organizations are not new. But what is new is that these attacks are on the increase and some have been successful in side-tracking, damaging, and weakening the organizations under attack. And, in a few instances, these attacks have resulted in the demise of social change organizations --think ACORN.

These attacks take many forms. The purpose of this memo is to name the various types of attacks and to share some stories/examples of these attacks.

Type of Attack	**Some Examples**
1. Accusations, complaints and/or investigations pertaining to violations of 501(c) 3 tax exempt status re: partisan activities, extensive lobbying/ exceeding lobbying limits), or unlicensed practice of law; or claims of misclassification of tax status e.g. are a union or a c(4)	-**Casa de Maryland**. Disgruntled politician caused highly trumped up "expose" of Casa leading to numerous investigations related to their tax-exempt status and nonpartisan civic activities. -**Workers right group in a southern state.** State attorney general inquiry regarding unlicensed practice of law because they provide workers' rights education and help workers who have experienced wage theft make claims against their employers.
2. Accusations, complaints and/or investigations related to misuse of government funding	-**Restaurant Opportunity Center's** (ROC United) use of a Department of Labor grant was challenged, no doubt, because ROC has effectively targeted the 3rd largest US industry. **-NTIC (now National People's Action)**, following an action by them on Karl Rove, extensive audit of Department of Justice grant. NPA has spent over $130,000, countless hours of staff time & 6 years defending themselves. Investigation still ongoing. Former director served prison time & house arrest.

3. Accusations, complaints and/or investigations of voter registration violations/fraud	-**Center for Civic Policy & South West Organizing Project** (NM) following an earth-shaking election that unseated that 4 long-time incumbents. -Most recently, **Florida New Majority** after FL went for Obama in 2012 -also **ACORN, One Arizona** & many others
4. Law suit(s) intended to censor, intimidate, financially burden or silence your organization or allies (strategic lawsuit against public participation=SLAPP suits)	--**Jobs with Justice** (JwJ) and faith leaders for supporting of workers in the Smithfield Food meatpacking plant. Smithfield Foods used the courts to intimidate & silence those publicizing dangerous conditions at Smithfield's packing plant in Tar Heel, North Carolina. They charged the union (UFCW) and JwJ with racketeering and other criminal charges. Included among the activities which Smithfield alleged criminal were: publishing a report about bad working conditions, passing resolutions calling on Smithfield to change, and speaking to the press. One such "threatening statement" was "'We've come here to send a message to Smithfield Foods while their board of directors and top executives gather to talk about their success and growth of the multibillion-dollar company. We want to remind them that there are people suffering every day in the largest meatpacking plant in the world.'"
5. Attempted entrapment/secret videotaping or audio recording	-**ACORN (**undercover sting operation/video-taping at several offices) -**Voces de la Frontera** (WI). FAIR, the well-known anti-immigrant group, sent plants wearing wires to try to illegally register to vote - **Coalition for Humane Immigrant Right**s. Highly edited secret taping made it appear that CHIRLA director was laughing during the pledge of allegiance.

6. Threats of physical intimidation, violence, hate calls/mail/stalking	- **Coalition for Humane Immigrant Right**s (CHIRLA) office has received bomb threats, has had white powder mailed to the director. A conservative talk radio station publicized the personal phone number of an employee asking viewers to call him. Director has been stalked/heckled, threatened by anti-immigrant activists. -**Voces de la Frontera** director has received threatening calls to her home and hate mail. Youth leaders doing "get out the vote" video-taped, harassed with intent to provoke. -**Southern Poverty Law Center**-threats of all sorts
7. Using "influence" to cut off support from friendly public & elected officials, allies, donors and foundation funders through misinformation, bullying, bribes, intimidation, and "divide and conquer tactics."	-**LA Alliance for a New Economy** was the subject of a massive public records request to local & state elected & office. The request came from a PR firm often hired by Karl Rove, Sarah Palin requiring hundreds of officials to turn over any & all communications they had had with LAANE. -**Sunflower Community Action** (KS) lost a large grant & many allies were "talked to" & harassed after they took action on their Secretary of State who is trying to move voter ID & makes many anti-immigrant statements
8. Character assassinations	-**Casa de Maryland, Voces de la Frontera** and others called "terrorist organizations", red-baited.
9. Attempts to access or delete confidential or important information such a donor lists, membership lists, databases, strategy documents.	-**America Comes Together** (the largest progressive Get Out the Vote organization operating in many swing states), had volunteers planted in the offices who successfully deleted their data bases & employee payroll records just prior to the 2004 national election -**A key, large national funder of ROC** had its email hacked; important information about ROC was obtained

Renewed Attacks on Worker Centers

Recently numerous worker centers including ROC United, The Korean Immigrant Worker's Alliance (KIWA) and others came under attack by the organization "The Center for Union Facts." The Center for Union Facts claims that worker centers are quasi union/fronts for unions and therefore should not be classified at 501c3 tax exempt organizations and should instead be classified at 501c5 organizations. C5 is the IRS designation for unions. As such, worker centers would also be subject to the same cumbersome reporting requirements placed on unions.

Increased Likelihood of Attack—Five Characteristics

We need to take these attacks or the potential of attacks very seriously. Social change/social justice groups with the following five characteristics are more likely to be targets of opposition attacks:

1) Is effective; having an impact
2) Is engaged in civic engagement/electoral work including nonpartisan voter registration, voter access issues, voter education and get out the vote efforts.
3) Is working in a swing state or on highly contested key national, state or local races
4) Is actively engaged on hot button issues such as reproductive justice, LGBTQ, labor/worker rights, immigration, health care reform.
5) Receives government funding (federal, state, or local)

Getting & Keeping the Organization's House in Order

One thing you will note which all these forms and examples of attacks have in common. *None of the attacks are about the substance of the issues the social change groups are working on.* The issues they are effectively working on are the reason for the attacks, but the attacks are all about finding or trying to find their vulnerabilities. And these vulnerabilities are most often internal to the organization. Thus, it is especially important that groups get and keep their internal house in order so as to minimize their risk and to minimize the damage potentially from these kind of below the belt opposition attacks. RoadMap's "Weathering the Storms" project is helping groups identify and address their vulnerabilities as well as helping them to create a crisis management plan that they can put into action when attacked. This way, with an "ounce of prevention," social change groups are better able to keep the focus of their work on the issues. And they are also ready and in a better position to confidently defend the actions and integrity of their organizations, when attacked.

This memo compiled by Mary Ochs of the RoadMap Weathering the Storm team.
September 16, 2013.
www.roadmapconsulting.org

PV Scale of Organization Data Health

Progressive Victory
Turning Data Into Power

Please answer by selecting 1 to 5, with 1 being false, or most negative, and 5 being true, or most positive.

1) My organization's list exists as one entity in a unified format.

1 2 3 4 5

2) List includes all contacts of sustained value for organization, except for those deliberately excluded for an explicit reason.

1 2 3 4 5

3) The list includes current and past board members, advisory or non-governance leaders (current and former), donors, lapsed donors, and donor prospects. *Consider all categories when answering this and next question.*

1 2 3 4 5

4) List also includes current and former activists and volunteers, current and former staff and consultants, allied elected and appointed public officials, former elected or appointed allied officials, and community allies (e.g., clergy, labor, business, academe, entertainment, artists, media, healthcare).

1 2 3 4 5

5) List has a designated organization staff custodian(s).

1 2 3 4 5

6) Organization has written standards of data access and control *and* privacy safeguards.

1 2 3 4 5

7) Passwords or access controls for organizational data are changed after transitions by staff, volunteers, or consultants with access to the data.

1 2 3 4 5

8) Staff custodian has in-depth knowledge of the list and its data structure.

1 2 3 4 5

9) If list is used or shared by partner organizations, the ownership and custody of the list are designated in writing. All parties communicate about that policy, including any changes to those designations.

1 2 3 4 5

10) Data entry for list abides by written standards of quality control.

1 2 3 4 5

11) Health, quality, and utility of the list are an articulated organizational priority.

1 2 3 4 5

12) List is backed up regularly with physical record stored in at least one secure, off-site location.

1 2 3 4 5

13) We have written procedure for backup and recovery, and—especially important—regular testing of recovery.

1 2 3 4 5

continued

14) My organization provides regular training for both data managers and data users, keeping skills up-to-date.

1 2 3 4 5

15) More than one staff person can access list at any given time.

1 2 3 4 5

16) Updates to the list, such as national change-of-address (NCOA) review, are conducted regularly (in the case of NCOA, for instance, quarterly updates of physical address are a requirement for bulk-mail discount).

1 2 3 4 5

17) If any update or process is conducted automatically, the organization receives and the list custodian maintains an electronic file and a written record of such reports or certifications resulting from the update.

1 2 3 4 5

18) Data selections or queries from the list can be retrieved quickly, within an hour (e.g., a phone list of donors, lapsed donors, and donor prospects in Atlanta).

1 2 3 4 5

19) Selections can be produced and shared in a variety of formats within a half-day, including call lists, e-mail lists, mailing lists or labels, and personal profiles or donor histories, full contact lists by city, ZIP, ZIP string or area, or state, or combinations of these (e.g., spreadsheet of donors, past donors, and prospects in 94*** Zip code string, in Bay Area of California).

1 2 3 4 5

20) A variety of relevant criteria can be selected interchangeably and the results produced in a variety of formats without stress or hassle (e.g., e-mail list for all past and present organization contacts in Maine; or phone and e-mail list for all records coded as volunteers who to date have not donated to the organization).

1 2 3 4 5

21) Prompt follow-up about new information or updates is a standard practice in the organization, initiated by senior staff or list custodian as a shared responsibility, with shared accountability and without blame.

1 2 3 4 5

22) Information learned and notated during contact or interaction with supporters gets reflected quickly and efficiently in the list.

1 2 3 4 5

23) Organization has incentives and rewards for maintenance and health of organization list and its growth.

1 2 3 4 5

24) Health, growth, and utility of the list are an explicit component of strategic planning by the organization.

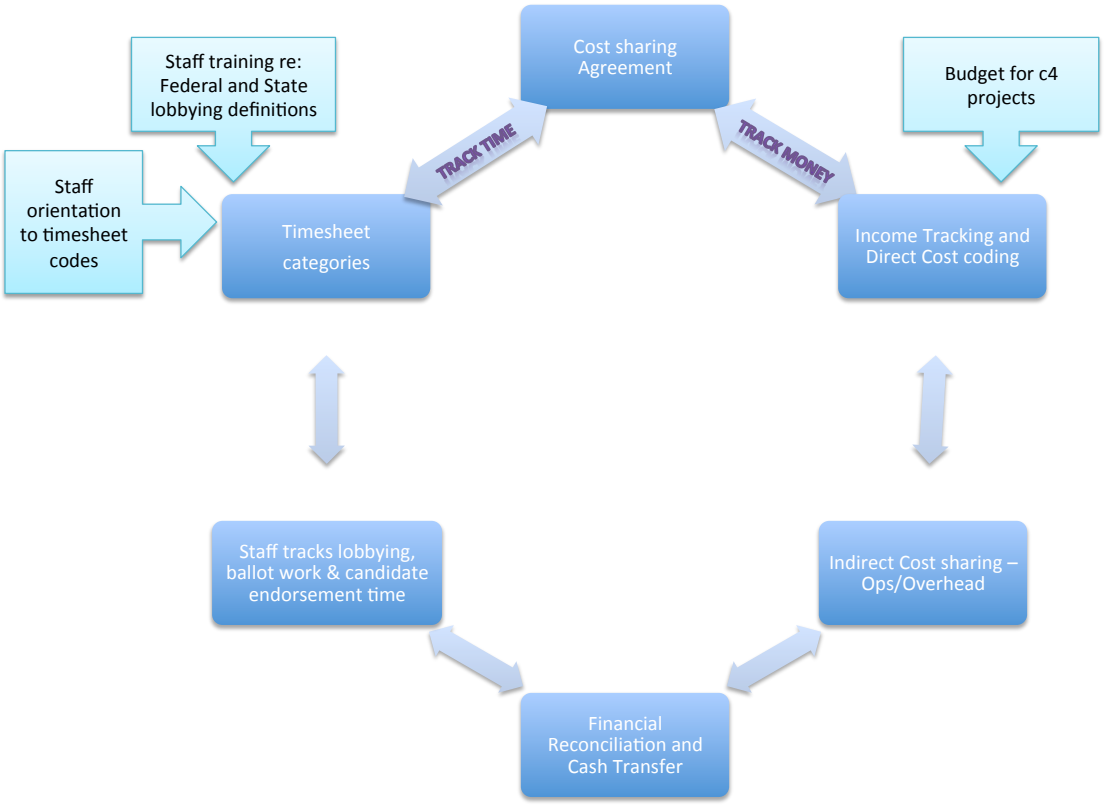
1 2 3 4 5

25) For any initiative the organization launches or adopts, acquisition and uses of new supporter data for the expansion of the list are part of that investment.

1 2 3 4 5

Add up scores. Any score of 75 or above is passing. Grade levels for scores are from 75 to 84: "D"; from 85 to 94: "C"; from 95 to 104: "B"; and 105 or above: "A." This exercise recommended for executive and *senior staff simultaneously. Scale is also useful as multi-year assessment. Revisit this tool annually and record your scores.*

C3 C4 Affiliated Organizations Transactions Flow Chart



Sample Acknowledgment of Ban on Nonpartisan Activities (c3 only)

(Name of Organization) recognizes and supports the rights and responsibilities of its employees, board members, and volunteers with regard to participation in the democratic process. (Name of Organization) employees are reminded that (Name of Organization) is a non-profit organization governed by Section 501(c) (3) of the IRS Code, and that participation in partisan campaigns (that is, campaigns in support of or opposition to a candidate for elected, public office) by such organizations are **strictly prohibited.** Therefore, if (Name of Organization) employees, board members, and volunteers choose to volunteer with such activities or campaigns, they must clearly identify themselves as individual volunteers rather than as (Name of Organization) representatives.

Contributions to political campaign funds, displaying materials in (fliers, buttons, stickers, posters) public statements of position (verbal or written) or other forms of endorsement such as appearances at rallies etc. made on behalf of (Name of Organization) in favor of or in opposition to any candidate for public office clearly violate the prohibition against political campaign activity. Conversely, you may not wear or display (Name of Organization) hats, buttons, t-shirts, materials etc. at partisan political functions. Violating this prohibition may result in denial or revocation of Name of Organization's) tax-exempt status and the imposition of certain excise taxes.

As an employee with (Name of Organization), you are prohibited from engaging in any of these activities while working during normal work hours. Should you wish to do so, you must request permission to be absent from work and you must use available leave time. Your time sheet must clearly reflect that you were not working during this time. You may not display any partisan material in the office or at (Name of Organization) meeting, events etc. You may not send or receive any email or other form of communication using (Name of Organization) resources or equipment (email address, computer, telephone etc.). If you engage in partisan activities during non-work hours you must make reasonable efforts to disassociate your participation from that of Name of Organization).

Employees should have a disclaimer in their use of social media that makes it clear that their views and opinions are their own and do not represent the views of (Name of Organization). Accordingly, an employee should not comment in such a manner unless there was a disclaimer or the employee was not being identified as being affiliated with (Name of Organization). Here is an example of appropriate disclaimer language: "The opinions expressed here are mine and not the opinions of my employer", or in the case of board members or volunteers "The opinions expressed here are mine and not the opinions of any organization whose board I may serve on or volunteer with."

I have received, read and understand (Name of Organization) "BAN on NONPARTISAN ACTIVITIES" policy and agree to strictly abide by this policy.

I understand that this signed receipt will be a part of my permanent personnel file.

_____Name

_____Signature

_____ Date

Sample Acknowledgment of Ban on Nonpartisan Activities (c3, c4)

(Name of Organization) recognizes and supports the rights and responsibilities of its employees, board members, and volunteers with regard to participation in the democratic process. (Name of Organization) employees are reminded that (Name of Organization) is a non-profit organization governed by Section 501(c) (3) of the IRS Code, and that participation in partisan campaigns (that is, campaigns in support of or opposition to a candidate for elected, public office) by such organizations are **strictly prohibited.** Therefore, if (Name of Organization) employees, board members, and volunteers choose to volunteer with such activities or campaigns, they must clearly identify themselves as individual volunteers rather than as (Name of Organization) representatives.

Contributions to political campaign funds, displaying materials in (fliers, buttons, stickers, posters) public statements of position (verbal or written) or other forms of endorsement such as appearances at rallies etc. made on behalf of (Name of Organization) in favor of or in opposition to any candidate for public office clearly violate the prohibition against political campaign activity. Conversely, you may not wear or display (Name of Organization) hats, buttons, t-shirts, materials etc. at partisan political functions. Violating this prohibition may result in denial or revocation of Name of Organization's) tax-exempt status and the imposition of certain excise taxes.

As an employee with (Name of Organization), you are prohibited from engaging in any of these activities while working during normal work hours. Should you wish to do so, you must request permission to be absent from work and you must use available leave time. Your time sheet must clearly reflect that you were not working during this time. You may not display any partisan material in the office or at (Name of Organization) meeting, events etc. You may not send or receive any email or other form of communication using (Name of Organization) resources or equipment (email address, computer, telephone etc.). If you engage in partisan activities during non-work hours you must make reasonable efforts to disassociate your participation from that of Name of Organization).

Employees should have a disclaimer in their use of social media that makes it clear that their views and opinions are their own and do not represent the views of (Name of Organization). Accordingly, an employee should not comment in such a manner unless there was a disclaimer or the employee was not being identified as being affiliated with (Name of Organization). Here is an example of appropriate disclaimer language: "The opinions expressed here are mine and not the opinions of my (Name of Organization)," or in the case of board members or volunteers, "The opinions expressed here are mine and not the opinions of any organization whose board I may serve on or volunteer with."

(Name of Organization) also has an affiliated organization which is a 501(c)4 called_____. (Name of 504(c)4 Organization) may engage in partisan political activities subject to federal and state campaign finance laws. If you are engaged in work with (Name of

504(c)4 Organization), you must be very careful to make it clear, at all times, you are working/speaking/acting on behalf of the (Name of 504(c)4 Organization) and not the 501(c)3.

I have received, read and understand (Name of Organization) “BAN on NONPARTISAN ACTIVITIES” policy and agree to strictly abide by this policy.

I understand that this signed receipt will be a part of my permanent personnel file.

_____Name

_____Signature

_____ Date

Sample Acknowledgment of Ban on Nonpartisan Activities (c3 only) (Spanish)

MUESTRA - Reconocimiento de la
PROHIBICIÓN DE ACTIVIDADES POLÍTICAS PARTIDISTAS
en (nombre de la organización) (solo c3)

(Nombre de la organización) reconoce y apoya los derechos y responsabilidades que tienen sus empleados, miembros de la mesa directiva y voluntarios de participar en el proceso democrático. Sin embargo, nombre de la organización es una organización designada como tipo 501(c)(3) que esta prohibida de participar en actividades electorales partidistas (o sea, campañas que apoyan o oponen a un candidato a un cargo público). Por lo tanto, si los empleados, miembros de la mesa directiva o voluntarios de nombre de la organización toman la decisión de participar en tales actividades políticas partidistas o campañas, deben identificarse como voluntarios individuales que no representan a nombre de la organización.

Los empleados de nombre de la organización no deben endosar públicamente, verbalmente o por escrito – en nombre de la organización – a ningún candidato a un cargo público, ni pueden representar a nombre de la organización en ningún evento del candidato. Contribuciones a fondos políticos de la campaña de un candidato, declaraciones de posición (ya sean verbales o por escrito) u otras formas de endosar a un candidato, tales como apariencias en mítines hechos en nombre de nombre de la organización a favor o en contra de un candidato a un cargo público son violaciones de la prohibición de actividad electoral en las campañas. Tampoco se debe usar o exhibir cachuchas, botones, camisetas o cualquier otros materiales de nombre de la organización durante una función política partidista. Una violación de esta prohibición podría resultar en la revocación del estatus oficial como organización sin fines de lucro con el fisco americano (IRS) y la imposición de ciertos impuestos de consumo.

Esta prohibido que los empleados de nombre de la organización promuevan la campaña de un candidato por un puesto partidista durante horas hábiles del negocio. Si lo quiere hacer, tiene que pedir permiso para estar fuera del trabajo usando sus horas de vacaciones u otro permiso. Su registro de asistencia (time sheet) debe reflejar que no esta trabajando durante esas horas. No debe colocar ningún material partidista en la oficina o en los eventos, juntas y otras reuniones de nombre de la organización. No debe mandar o recibir ningún correo electrónico partidista u otra forma de comunicación usando los recursos o equipo de nombre de la organización (dirección de correo electrónico, computadora, teléfono, copiadora, etc.). Si recibe un mensaje partidista en su buzón de correo electrónico de nombre

de la organización, avise de inmediato al remitente que su mensaje ha llegado a un correo electrónico del trabajo de nombre de la organización, que es una organización no partidista. Debe pedirle que deje de usar esta dirección de correo electrónico para contactarle a Ud. Si quiere seguir recibiendo correos electrónicos de ese remitente, favor de darle otro correo electrónico no relacionado con nombre de la organización. Si Ud. participa en actividades partidistas fuera del trabajo, debe esforzarse a romper cualquier conexión entre esa actividad y su trabajo con nombre de la organización.

Para cumplir con la "Política de Tecnología y Medios Sociales" de nombre de la organización, los empleados y miembros de la mesa directiva deben poner una cláusula de exención de responsabilidad en sus comunicaciones por medios sociales que aclara que sus puntos de vista y opiniones son de ellos mismos y no representan el punto de vista de nombre de la organización. Por lo tanto, un empleado no debe hacer un comentario de ese tipo, al menos que haya esa cláusula de exención de responsabilidad o si el empleado no este identificado como afiliado con nombre de la organización. Éste es un ejemplo del lenguaje apropiado para una declaración: "Las opiniones expresadas aquí son mías y no necesariamente las opiniones de nombre de la organización."

Si tiene preguntas acerca de esta política, o necesita ayuda para escribir un mensaje no-partidista o una cláusula de exención de responsabilidad, favor de ponerse en contacto con _____ de inmediato.

He recibido, leído y comprendido la PROHIBICIÓN DE ACTIVIDADES POLÍTICAS PARTIDISTAS y estoy de acuerdo en mantener estrictamente esta política. Entiendo que una violación de esta política puede resultar en acciones disciplinarias, incluyendo la terminación del trabajo (para empleados) y terminación de servicio en la mesa directiva (para los directores voluntarios).

Entiendo que este recibo firmado por mí se incorporará en mi archivo permanente de personal.

_____Nombre (letra de molde)

_____Firma

_____Fecha

Sample Acknowledgment of Ban on Nonpartisan Activities (c3, c4) (Spanish)

MUESTRA - Reconocimiento de la
PROHIBICIÓN DE ACTIVIDADES POLÍTICAS PARTIDISTAS
en (nombre de la organización) (c3 y c4)

(Nombre de la organización) reconoce y apoya los derechos y responsabilidades que tienen sus empleados, miembros de la mesa directiva y voluntarios de participar en el proceso democrático. Sin embargo, nombre de la organización es una organización designada como tipo 501(c)(3) que esta prohibida de participar en actividades electorales partidistas (o sea, campañas que apoyan o oponen a un candidato a un cargo público). Por lo tanto, si los empleados, miembros de la mesa directiva o voluntarios de nombre de la organización toman la decisión de participar en tales actividades políticas partidistas o campañas, deben identificarse como voluntarios individuales que no representan a nombre de la organización.

Los empleados de nombre de la organización no deben endosar públicamente, verbalmente o por escrito – en nombre de la organización – a ningún candidato a un cargo público, ni pueden representar a nombre de la organización en ningún evento del candidato. Contribuciones a fondos políticos de la campaña de un candidato, declaraciones de posición (ya sean verbales o por escrito) u otras formas de endosar a un candidato, tales como apariencias en mítines hechos en nombre de nombre de la organización a favor o en contra de un candidato a un cargo público son violaciones de la prohibición de actividad electoral en las campañas. Tampoco se debe usar o exhibir cachuchas, botones, camisetas o cualquier otros materiales de nombre de la organización durante una función política partidista. Una violación de esta prohibición podría resultar en la revocación del estatus oficial como organización sin fines de lucro con el fisco americano (IRS) y la imposición de ciertos impuestos de consumo.

Esta prohibido que los empleados de nombre de la organización promuevan la campaña de un candidato por un puesto partidista durante horas hábiles del negocio. Si lo quiere hacer, tiene que pedir permiso para estar fuera del trabajo usando sus horas de vacaciones u otro permiso. Su registro de asistencia (time sheet) debe reflejar que no esta trabajando durante esas horas. No debe colocar ningún material partidista en la oficina o en los eventos, juntas y otras reuniones de nombre de la organización. No debe mandar o recibir ningún correo electrónico partidista u otra forma de comunicación usando los recursos o equipo de nombre de la organización (dirección de correo electrónico, computadora, teléfono, copiadora, etc.). Si recibe un mensaje partidista en su buzón de correo electrónico de nombre de la organización, avise de inmediato al remitente que su mensaje ha llegado a un correo electrónico del trabajo de nombre de la organización, que es una organización no partidista. Debe pedirle que deje de usar esta dirección de correo electrónico para contactarle a Ud. Si quiere seguir recibiendo correos electrónicos de ese remitente, favor de darle otro correo electrónico no relacionado con nombre de la organización. Si Ud. participa en actividades partidistas fuera del trabajo, debe esforzarse a romper cualquier conexión entre esa actividad y su trabajo con nombre de la organización.

Para cumplir con la "Política de Tecnología y Medios Sociales" de nombre de la organización, los empleados y miembros de la mesa directiva deben poner una cláusula de exención de responsabilidad en sus comunicaciones por medios sociales que aclara que sus puntos de vista y opiniones son de ellos mismos y no representan el punto de vista de nombre de la organización. Por lo tanto, un empleado no debe hacer un comentario de ese tipo, al menos que haya esa cláusula de exención de responsabilidad o si el empleado no este identificado como afiliado con nombre de la organización. Éste es un ejemplo del lenguaje apropiado para una declaración: "Las opiniones expresadas aquí son mías y no necesariamente las opiniones de nombre de la organización."

Si tiene preguntas acerca de esta política, o necesita ayuda para escribir un mensaje no-partidista o una cláusula de exención de responsabilidad, favor de ponerse en contacto con _____ de inmediato.

(NOMBRE DE LA ORGANIZACIÓN) también tiene una organización afiliada que es una organización tipo 501(c)4 llamada _____. (NOMBRE DE LA ORGANIZACIÓN 501(c)4) puede participar en actividades políticas partidistas bajo las leyes federales y estatales sobre finanzas en las campañas políticas. Si Ud. participa en el trabajo de (NOMBRE DE LA ORGANIZACIÓN 501(c)4), debe hacer todo lo posible para aclarar, en toda ocasión, que esta trabajando/hablando/actuando en representación de (NOMBRE DE LA ORGANIZACIÓN 501(c)4) y no de la organización 501(c)3.

He recibido, leído y comprendido la PROHIBICIÓN DE ACTIVIDADES POLÍTICAS PARTIDISTAS y estoy de acuerdo en mantener estrictamente esta política. Entiendo que una violación de esta política puede resultar en acciones disciplinarias, incluyendo la terminación del trabajo (para empleados) y terminación de servicio en la mesa directiva (para los directores voluntarios).

Entiendo que este recibo firmado por mí se incorporará en mi archivo permanente de personal.

_____Nombre (letra de molde)
_____Firma
_____Fecha

How Worker Centers Can Keep 501c3 Tax Exempt Status

by Brian Glick, who directs a Fordham Law School program that represents several major worker centers

Worker centers' 501c3 tax exempt status has recently come under attack. The attackers claim that worker centers are not entitled to 501c3 status because "they are unions under another name."

These attacks are part of a broader campaign against worker centers. That campaign shows that business interests are worried because worker centers are becoming effective.

The key response is for worker centers to intensify their main work and not be diverted or distracted by these attacks. At the same time, it may help to clarify why the attacks are wrong and what worker centers can do to protect 501c3 status. [2]

Why 501c3 status is important

501c3 status makes a contribution to a worker center deductible from the donor's taxable income. It makes it easy for foundations to give grants directly to worker centers. (Foundations can give grants in other ways, but those ways are difficult and not readily available). Though there are other forms of exemption from federal income tax, only 501c3 facilitates foundation grants and makes contributions tax deductible.

Why worker centers are entitled to 501c3 status

501c3 status is for non-profit organizations that qualify as "charitable" or "educational." "Charitable," under tax law, does not mean giving away money. It is IRS-speak for providing a public benefit.

Worker centers fight to make life better for all workers in an industry or a community. Their activities fall well within IRS guidelines. Under IRS rules, a group qualifies for 501c3 if all or almost all of its activities aim to:

Advance civil and human rights under law

[2] The attackers also argue that worker centers should be subject to the National Labor Relations Act and the Labor Management Disclosure & Reporting Act, which govern and restrict union organizing. A helpful overview of that issue, with guidance on how to avoid those laws, is "Worker Centers and Traditional Labor Law: How to Stay on the Good Side of the Law," nlg-laboremploy-comm.org/.../ProjWkrCtr_2010

Combat discrimination

Improve public health and social welfare

Provide research and public education on subjects beneficial to the community

Provide instruction or training for individuals for purposes of improving their capacities

Help people who are “poor and distressed” or “under-privileged”

Why worker centers get different tax status from labor unions

Labor unions do not get 501c3 status. They get 501c5 status, which exempts them from federal income tax but does not make contributions deductible or facilitate foundation grants.

Labor unions do not get 501c3 status because they are "mutual benefit" organizations. A labor union is required by law to serve the interests of a defined, limited groups of workers, mainly members, and to be responsible only to them.

A worker center, by contrast, is a "public benefit" organization. It does not serve only a limited set of people. Its activities benefit all of the workers in an industry or neighborhood. It may have no members or only a small membership of activists who work for goals far beyond the self-interest of those activists. If a worker center has members, membership is open to any worker in a particular industry or neighborhood who wants to help.

How worker centers can protect their 501c3 status

1. Make it clear that all activities are part of efforts to help a broad, open-ended set of workers and their communities. Often a worker center helps an individual or a small group of workers to deal with a particular abuse, such as wage and hour violations, racial discrimination, sexual harassment or unsafe working conditions. When doing that, make it clear that such efforts are not just for the personal benefit of the workers involved, but are an integral part of broad initiatives to improve the lives of a very large group of people who are poor, distressed or under-privileged.

This frame is valuable politically. It is also essential legally, to show that the worker center is not operating for the "private benefit" of individuals or the "mutual benefit" of worker center members or any other small limited group. This frame should be emphasized in all the worker center's literature, handouts, leaflets and talking points. It should be all over the center's website and Facebook page, and it should be explicit in the center's annual federal income tax return (Form 990, discussed in #8).

2. Keep membership open-ended and indefinite. Many worker centers have identified the need to build a broad, dues-paying membership base. It is fine for a 501c3 organization to have members, so long as it works to benefit a large group of workers who need help. Services (such

as job training or help with wage theft or other law violations) can be available only to members, so long as any low-wage worker in the industry or neighborhood who supports the goals of the organization can easily join. Before initiating a major program of member benefits or restricting services only to dues-paying members, consult with a knowledgeable lawyer or advisor to minimize risk to your 501c3 status.

3. When protesting against a particular employer, make it clear that the center is not seeking to become collective bargaining agent for the employer's workers or to benefit only those workers. It is fine to run a campaign – with pickets, lawsuits, whatever – against a particular employer as part of your broader efforts But make it clear in every way you can that you are not a labor union and you do not seek to gain recognition as the workers' collective bargaining agent. (This helps address labor law as well as 501c3 concerns.) Stress that your work is not just for those workers, but is part of your effort to improve the lives of all the workers in your industry or neighborhood. Also, if your organization contemplates supporting or promoting civil disobedience or other law violation, consult first with a sympathetic lawyer or other advisor in order to make sure your do not risk losing 501c3 status.

4. Any labor union formed by workers you are helping should be a legally independent organization separate from the worker center. It's fine for workers of a particular employer to organize and negotiate with that employer for improved wages and working conditions on an ongoing basis (rather than to resolve a single lawsuit or campaign). But they should not carry out that activity within a worker center or other 501c3 organization. You can help the workers to understand their rights and assess their options. If they want, you can help them to affiliate with a larger union or form their own union. If the employer obstructs their efforts or retaliates against them, you can help defend the workers' freedom to exercise their legal rights. Any union the workers form or join will be entitled to 501c5 status, but not 501c3.

5. It is fine to collaborate and coordinate with a labor union, but do not subsidize the union or act as its agent.

Worker centers and labor unions share many objectives. It is very often in their mutual interest, and potentially of great benefit to workers, for them to cooperate and collaborate in a range of ways. Most such collaboration is fine under 501c3 law, but centers need to be careful to avoid certain relationships that could risk 501c3 status.

It is fine under 501c3 law for a worker center to accept funding from a labor union and to include some labor union representatives on its board of directors. But a center risks losing 501c3 status if it cedes control to the union and functions as its agent, for example if the union has a majority of seats on the center's board or power to hire, fire, discipline or supervise its staff, or if e-mails, meeting notes, etc. show that the worker center is in fact taking direction from the union rather than making its own decisions.

It is fine under 501c3 law for a worker center to share office space and resources with a union, so long as the worker center is reimbursed at market rates. But a 501c3 worker center cannot

fund a labor union or help it in ways that amount to a subsidy. Within those limits, it is fine under 501c3 law to collaborate with a labor union on policy or legislative campaigns and in efforts to mobilize and support unorganized workers. It is best to carefully plan the details of such collaboration in discussion with friendly lawyers or other advisors.

6. Do not support candidates for elected office. A 501c3 organization can engage in non-partisan activities such as voter registration and education or get out the vote drives, so long as you do not in any way support a particular candidate in any election at any level of government.

7. Keep legislative advocacy expenditures within IRS limits. Worker centers should choose to be governed by the expenditure test (IRS form 5768). That test limits "attempts to influence legislation" to up to 20% of your annual budget (a little less if the center's income is over $500,000). It imposes much lower limits (5%, or less as income increases) on what IRS calls "grassroots lobbying," efforts to persuade and help other people, who are not actively involved with the center, to try to influence legislation. Be sure to keep very careful records, especially of paid staff time. For complicated questions consult the Alliance for Justice website or staff.

Remember: Issue advocacy not connected with legislation is unrestricted. So is lobbying any official for government action that is not linked to legislation. So is activity by your staff which is outside paid time and does not use the center's name or resources.

Remember also that some states and localities have separate registration and disclosure requirements for groups that lobby, and that those laws may define lobbying more broadly than IRS.

8. Pay close attention to federal income tax returns (IRS Form 990); do not just hand them off to your accountant. The financial information in your annual return needs to be accurate and detailed, especially regarding legislative advocacy. Form 990 also requires that every 501c3 organization re-state its mission and provide a narrative of its major programs or projects during the tax year.

IRS reads this to make sure you still qualify for 501c3 status. Opponents of worker centers also read 990s. Each 990 is public record. It's available on Guidestar and other websites. You are required to make a copy promptly available to anyone who asks for it.

So, do not just turn your 990 over to your accountant. Check all figures and entries carefully. Draft your mission statement and program narratives yourselves, with help and review by a supportive lawyer or other advisor. Make sure the statement and narratives stress the broad public benefits provided by all worker center activities.

FOR FURTHER GUIDANCE & ADVICE:
To better prepare for and cope with opposition attacks, Road Map Consulting, www.roadmapconsulting.org, offers materials and consulting on strategic planning and capacity

building and **has a special project that assists with preventing, protecting and preparing for opposition attacks.**

On advocacy, lobbying, and political activity, the Bolder Advocacy program of Alliance for Justice, www.bolderadvocacy.org posts a broad range of practical, accessible, updated materials and provides workshops and trainings, as well as one-on-one technical assistance.

For official government policies and forms, you can learn a great deal from the easily navigated IRS website, http://www.irs.gov/Charities-&-Non-Profits.

On 990 Federal income tax returns, Guidestar.com.

For legal advice and assistance check out local legal services offices, law school clinics, and public interest law centers (such as Lawyers Alliance and Urban Justice Center in NY, Public Counsel and Insight Center for Community Economic Development in CA, other groups listed at http://www.lawyersalliance.org/ProvidersNat.php). Get referrals from a friendly labor lawyer or the local chapter of the National Lawyers Guild. You may also be able to get free assistance from a sympathetic lawyer working at a major law firm.

Disclaimer: The information in this memo is not intended to be legal advice. We recommend you consult a qualified legal advisor regarding legal requirements that affect your nonprofit organization's fundraising activities. Further, regulations change from time to time so consult the appropriate regulatory bodies for current requirements.

Fundraising—Charitable Solicitation in Multiple States Registration and Compliance

Fundraising activities are regulated primarily by state law. Most states require charitable nonprofit organizations to register with the state usually before soliciting donations. Registration usually includes payment of a fee. Most states have an annual registration and reporting requirements. Charitable fundraising is usually regulated by either the state's Attorney General or Secretary of State. Check the website of the state's Attorney General or Secretary of State Charitable Division to learn all of the requirement that apply to your fundraising activities.

Currently, thirty-eight state and the District of Columbia have registration requirements. Eight states do not have charitable solicitation statutes and, therefore, do not require any form of registration or reporting. Currently, they are Delaware, Iowa, Idaho, Indiana, Nebraska, Vermont, South Dakota and Wyoming. Four states have statutes that exempt some types of nonprofits from registering. These include Arizona, Texas, Missouri and Louisiana. The later only requires registration if the nonprofit hires professional fundraising consultants to engage in solicitation.

Generally, you are required to registration before engaging in a solicitation campaign. However, California has a requirement that you must register 30 days after you receive your first charitable donation (grant, corporate contribution, government grants etc.).

Check the state statutes to make sure you are compliant and to learn of any exemptions that may apply to your fundraising activity.

Most of these states also regulate and require paid fundraising consultants to register also. If you utilize the services of a paid fundraising counsel or consultants who you hire you should check you state law and check to make sure your consultant is compliant.

Soliciting Funds in Multiple States

States are increasingly taking fundraising registration seriously. Lack of compliance can trigger fines, reputational damage or worse. If you are soliciting funds in multiple states be it via a donate button on electronic communications, direct mail, phone solicitations or personal "asks" or other activity that asking for a donation then it is likely that this activity will require you to register in each state for which you are engaging in solicitations. This is an evolving area of regulation. Many of the state statutes were created before online communications and fundraising become common. Just the existence of a donate button probably does not trigger registration in every state you may be soliciting or receiving donations.

But if you are following up on the donors or names you are collecting on line then that activity is likely to be considered solicitation. We recommend you err on the side of caution and register.

Disclosure Statements

In addition to registration, organizations may need to publish standard disclosure statements to the donors. About half the states require some form of disclosure statements which are disclosures as to where a donor can find more information about the soliciting organization either from a governmental agency or the organization's website or both. The specific disclosure language requirements vary from state to state.

The Harbor Compliance site has a good review of the 'disclosure' requirements that organizations may need to provide when doing. https://www.harborcompliance.com/information/charitable-solicitation-disclosures

Games of Chance
Please note that holding fundraising events or games of chance often have additional regulations from the states as well at the local communities in which events are conducted.

Penalties
States can and will impose penalties for noncompliance with fundraising registration and reporting requirements. These vary from fines to disallowing fundraising activities. Some states have been lax in monitoring but as more states seek increased revenue sources we have seen more emphasis on monitoring and compliance of state requirements such as fundraising registration

Getting It Done!

Some nonprofits hire the accountant/CPA that prepares the nonprofit's IRS 990 to also prepare and submit state charitable registration forms, since much of the information required by states for charitable registration is the same information that the nonprofit reports on its annual report to the IRS, Form 990. Other nonprofits outsource this project to a firm that specializes in preparing state registration forms. Still other nonprofits prepare the forms using internal staff.

For nonprofits seeking to file charitable registration forms in all the states where registration is required, the cost of filing fees plus labor for preparation of the forms can be very costly.

Many states require not only an initial registration but ongoing registrations in subsequent years. There may be late fees apply, so be sure to note renewal deadlines.

Here are some options to assist you in complying with registration requirements. They range from contracting firms that will register your nonprofit to self-help resources such as Nolo Press.

http://www.nationalcorp.com/ncr/solutions/Nonprofit-Services/Charitable-Solicitation-Registration-and-Renewal-Services

http://www.labyrinthinc.com

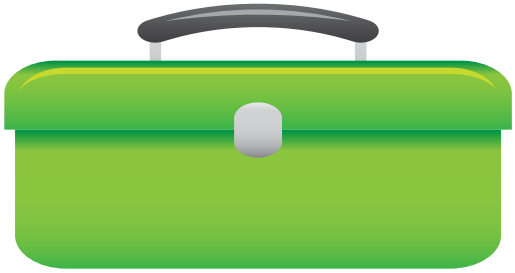
www.simplecharityregistration.com

Nonprofit Fundraising Registration, Nolo's 50-State Digital Guide. Nolo's new *50-State Digital Guide* provides everything you need to handle registration on your nonprofit. Self help guide Nolo Press. www.nolo.com

Resources:

- Find the states that regulate charitable registration from this map.
- Find your state agency responsible for regulating fundraising activities. The charity official varies from state to state.
- Forms and requirements for registration and reporting vary from state to state. Use this link to identify the websites of the regulatory agencies in states in which you are soliciting donations. Find your state's charity official for more information.
- Games of chance may require registrations or additional registrations also.

Section 6: Must Read Resources, Websites and Email Addresses



Your **TOOLKIT** items in this section include resources offered by a wide range of organizations and valuable websites.

6.1 Must Read Resources
6.2 Helpful Websites and Contacts
6.3 My Healthy Organization

The Must Read Resource Listing

There is an abundance of additional resources available to help you protect your organization against opposition attacks. In particular, the Alliance for Justice and Political Research Associates are two organizations that have long been supporting non-profits in legal compliance and opposition research and preparedness, respectively. We list some of their resources here.

Check back periodically, as we will continue to update the toolkit and this list of resources as additional information comes to our attention. You can download our presentation, the *must read* resources, and sample policies at http://www.roadmapconsulting.org/index.php/protecting-against-opposition-attacks. Please contact meredith@roadmapconsulting.org to access the password.

Record Keeping and Confidentiality

- "Keeping Track: A Guide to Record Keeping for Advocacy Charities" by Alliance for Justice
- "Sample Confidentiality Agreements" by National Council on Nonprofits

Lobbying

- "Influencing Public Policy in the Digital Age" by Bolder Advocacy
- "Private and Public Foundations May Fund Public Charities that Lobby" by Bolder Advocacy
- "Election Checklist for 501(c)(3) Charities" by Bolder Advocacy
- "Shaping the Future: A Compliance Guide for Nonprofits Influencing Public Policy in California" by Bolder Advocacy
- "Maximizing Your Lobbying Limit by Electing to Use the 501(h) Expenditure Limit" by Bolder Advocacy
- "State Lobbying Registration Thresholds" by Bolder Advocacy
- "Influencing Public Policy in the Digital Age: The Law of Online Lobbying and Election-related Activities" by Bolder Advocacy

Funders

- "Tips for Funders Preparing for the Possibility of a Politically Motivated Attack" by Bolder Advocacy

General Security Measures

- "Common Sense Security" by Political Research Associates

990s and Financial Management

- "How to Read the 990" by Nonprofit Coordinating Committee
- "Give Me Your 990! Public Disclosure Requirements for Tax-Exempt Organizations" by Alliance for Justice
- "How to Make the 990 Work for You" by Guidestar
- "State Law Nonprofit Audit Requirements" by the Council of Nonprofits

Affiliated 501(c)(3) and 501(c)(4) Organizations

- "The Practical Implications of Affiliated 501(c)(3) and 501(c)(4) Organizations" by Bolder Advocacy

Social Media

- "Tips on Using Social Media for Advocacy" by Bolder Advocacy

The RoadMap Resource Library assembles helpful documents in a number of categories. You can see additional resources organized by topic at http://www.roadmapconsulting.org/resource-library.

Helpful Websites and Contacts

Fun with Financials – http://www.funwithfinancials.net

MAP for Nonprofits – http://www.mapfornonprofits.org

Political Research Associates – http://www.publiceye.org

Financial Accounting Standards Board – http://www.fasb.org

Alliance for Justice – http://www.bolderadvocacy.org

Abby Levine – abby@afj.org

Camino PR – http://www.caminopr.com

Andrea Hagelgans – ahagelgans@caminopr.com

RoadMap – http://www.roadmapconsulting.org

Elsa Ríos, Co-Director (East Coast) – elsa@roadmapconsulting.org

Emily Goldfarb, Co-Director (West Coast) – emily@roadmapconsulting.org

Request Services – http://www.roadmapconsulting.org/apply-for-services

Harmon, Curran, Spielberg + Eisenberg, LLC – http://www.harmoncurran.com/

Beth Kingsley – bkingsley@harmoncurran.com

My Healthy Organization Online Assessment Tool -- www.myhealthyorganization.org

My Healthy Organization

An Online Assessment Tool for Social Justice Organizations

Be proactive in insulating your organization against attacks. Just as you plan ahead to protect yourself against stormy weather and unpredicted environmental changes, your organization requires similar appraisal and preparation. Completing periodic organizational assessments can improve performance; increase organizational learning; facilitate alignment around mission, vision, and values; assist in better delivery of programs; and steady your daily operations.

RoadMap offers this online tool, My Healthy Organization (MHO), which is an ideal assessment tool for organizations that are seeing a changed political landscape and needing to plan for this new reality and may be a useful companion process to the checklist you will find in this toolkit. It is a comprehensive organizational assessment tool created specifically for use by social justice organizations, and for organizations that blend social justice work with the provision of social services. Many of the issues we have discussed in this toolkit and on the webinar are captured in MHO, along with many others. It is available in English and in Spanish.

MHO is rooted in the values and practice of social change groups. It is one of the few organizational development tools that take into account dynamics of race, class and gender, and that explore underlying power dynamics within organizations. MHO is also unique in the sense that it is based on the value that organizational development doesn't belong in a silo, and that everyone within an organization has the right to know and offer their opinions and insights into organizational development issues.

MHO offers all participants the opportunity to think about the importance of organizational assessment, characteristics of movement-building organizations, and introduces the concept of organizational life cycle that can allow groups to not only assess where they are currently but also where they would like to go.

MHO covers eight areas of organizational assessment:

1. Purpose: Mission, Vision, Values
2. Priorities and Planning
3. Structures and Practices for Leadership & Management
4. People: ED, Staff, Board, Volunteers
5. Systems
6. Evaluation and Quality
7. Organizational Culture and Relationships
8. Community Engagement and Accountability

Learn more at www.myhealthyorganization.org

my Healthy Organization

The tool that strengthens your organization, community, movement

MHO allows you to:

- Assess your organization's stage of development
- Involve everyone in your organization in a process of reflection and analysis
- Tabulate results to help you identify strengths and areas for improvement
- Kickstart honest discussions and develop strategic next steps

Specifically designed for social change organizations, and for organizations that blend social services and social change…

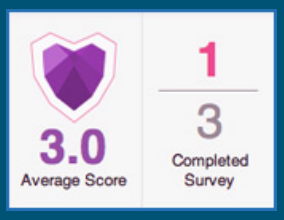
My Healthy Organization is an ideal assessment tool for organizations that are:

- Kicking off strategic planning and wanting to begin with a snapshot of strengths and challenges
- Needing to reassess in the face of a leadership transition or funding loss or gain
- Seeing a changed political landscape or community, and needing to plan for this new reality

www.myhealthyorganization.org

For information, contact Alfreda Barringer: alfreda@roadmapconsulting.org

MHO Assessment Tool Features:

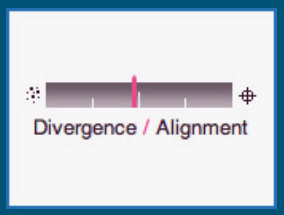


Measured results

As each person completes the assessment survey, MHO automatically tallies & scores their responses for you to capture valuable information.

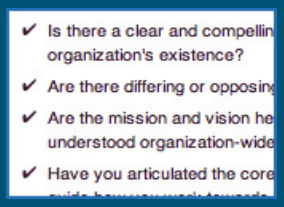
Detailed reports

MHO provides detailed reports featuring easy to read graphs and sortable tables that enable leaders and stakeholders to easily view and understand your assessment results.



Alignment/Divergence

Quickly see if individuals in your organization are in agreement or have differing responses with MHO's easy to read alignment meter.



Suggestions/analysis

Depending on your organization's average score in the 8 areas of organizational life, specific suggestions and analysis are provided, helping you understand how to use the information to make your next move.

Building Organizations, Communities and Social Movements

My Healthy Organization is specifically designed for social change organizations, and for organizations that blend social change work with the provision of social services.

www.myhealthyorganization.org

MHO is a project of ***RoadMap****. Strengthening organizations. Advancing social justice.*