



Weathering the Storms

A Toolkit on Protecting Your Organization
Against Opposition Attacks
April 2018

Not for Public Distribution

Table of Contents

Welcome	5
Introduction and Purpose	5
Acknowledgments	6
About RoadMap	7
Section 1: Getting and Keeping Your House in Order	8
A Guide to Getting and Keeping your House in Order	10
Working with Funder Allies.....	25
Best Practices for an Ethical Organization	28
Super Prepared Organization Sample Crisis Management Plan	30
Section 2: Crisis Communications	33
Introduction	34
Crisis Communications Strategy Plan	34
Crisis Communications Risk Assessment Tool.....	37
Crisis Communications Knowledge Checklist.....	39
Crisis Communications Infrastructure Checklist	40
Sample Crisis Communications Plan: Civic Engagement Scenarios.....	44
Sample Social Media Policy.....	47
Section 3: Key Organizational Policies.....	49
Introduction	50
Sample Compliance Calendar.....	51
Elements of a Crisis Management Plan	52
Sample Board of Directors Minutes	55
Sample Board of Directors Conflict of Interest Policy	56
Sample Confidentiality Statement	60
Sample Confidentiality Statement (Spanish)	61
Sample Incident Report Form	62
Sample Whistleblower Policy.....	65
Sample Litigation Hold Policy.....	67
Sample Document Retention and Destruction Policy	69
Corporate Attacks: Limit your Risk.....	71
Volunteer Screening and Protocol	74
Sample Intern & Volunteer Questionnaire	75
Sample of Volunteer Handbook Table of Contents.....	77
Sample Confidentiality Agreement for Volunteers.....	78
Independent Contract definition, checklist and questions.....	79
Harassment Bullying Sample Policy.....	82
Section 4: Digital & Data Security	85
Digital Security in a Nutshell	86
Digital Security Checklists Version 2.1.....	89
Digital Security Readiness Assessment Tool.....	90
Directions and Legend	94
Device Security Checklist.....	97
Password and Authentication Safety Checklist	104
Wireless Network Safety Checklist	109

Email Safety Checklist	113
G Suite Security Checklist	120
Appendix A: Digital Security Glossary	128
Appendix B: Assumed Threat Model	130
Appendix C: Frequently Asked Questions.....	134
Constitutional Communications Strategic Security Planning	137
Scale of Organization Data Health Tool	153
Glossary	155
Section 5: Creating Community & Office Safety	157
Office Security Series: Entrapment Prevention and Preparation.....	158
De-escalation Methods and Tactics	159
Tips on Creating Office Safety Protocols	163
Office Safety Sample Inventory	166
Office Safety Planning Worksheet.....	168
Entrapment Protection.....	171
Creating a Community Security Plan for Actions, Events, and Demonstrations	177
Section 6: Various Memos, Tools and Documents.....	180
Understanding and Beating Back Opposition Attacks Memo.....	181
C3 C4 Affiliated Organizations Transactions Flow Chart	185
Sample “Cost Sharing Agreement”	186
Sample Acknowledgment of Ban on Nonpartisan Activities (c3 only)	191
Sample Acknowledgment of Ban on Nonpartisan Activities (c3, c4)	192
Sample Acknowledgment of Ban on Nonpartisan Activities (c3 only) (Spanish).....	194
Sample Acknowledgment of Ban on Nonpartisan Activities (c3, c4) (Spanish)	196
How Worker Centers Can Keep 501c3 Tax Exempt Status	198
Fundraising—Charitable Solicitation in Multiple States Registration and Compliance	202
Section 7: Must Read Resources, Websites and Email Addresses	205
The Must Read Resource Listing	206
Helpful Websites and Contacts	208
My Healthy Organization	209
Getting IT Support for Your Organization.....	212

Table of Figures

Figure 1 - A Guide to Getting and Keeping your House in Order Checklist. Updated July 2017	10
Figure 2 - Emergency Phone Tree	32
Figure 3 - Crisis Communications Strategy Plan	34
Figure 4 - Crisis Communications Risk Assessment Tool	37
Figure 5 - Crisis Communications Knowledge Checklist	39
Figure 6 - Crisis Communications Infrastructure Checklist.....	40
Figure 7 - Crisis Communications Plan: Civic Engagement Scenarios Sample Template.....	44
Figure 8 - Social Media Policy.....	47
Figure 9 - Sample Compliance Calendar.....	51
Figure 10 - Elements of a Crisis Management Plan	52
Figure 11 - Sample Board of Directors Minutes	55
Figure 12 - Sample Board of Directors Conflict of Interest Policy	56
Figure 13 - Sample Confidentiality Statement	60
Figure 14 - Sample Confidentiality Statement (Spanish)).....	61
Figure 15 - Sample Incident Report Form	62
Figure 16 - Sample Whistleblower Policy	65
Figure 17 - Sample Litigation Hold Policy	67
Figure 18 - Sample Document Retention and Destruction Policy	69
Figure 19 - Sample Intern & Volunteer Questionnaire.....	75
Figure 20 - Sample of Volunteer Handbook Table of Contents.....	77
Figure 21 - Sample Confidentiality Agreement for Volunteers	78
Figure 22 - Independent Contractor Checklist	81
Figure 27 - Constitutional Communications Strategic Security Planning	137
Figure 28 - Threat Matrix	142
Figure 29 - Compartmentalization Strategy	143
Figure 30 - Workflow Security Level.....	144
Figure 31 - Scale of Organization Data Health Tool.....	153
Figure 32 - Office Safety Sample Inventory	166
Figure 33 - Office Safety Planning Worksheet.....	168
Figure 34 - C3 C4 Affiliated Organizations Transactions Flow Chart	185
Figure 35: Sample C3-C4 "Cost Sharing Agreement"	186
Figure 36 - Sample Acknowledgment of Ban on Nonpartisan Activities (c3 only)	191
Figure 37 - Sample Acknowledgment of Ban on Nonpartisan Activities (c3, c4).....	192
Figure 38 - Sample Acknowledgment of Ban on Nonpartisan Activities (c3 only) (Spanish).....	194
Figure 39 - Sample Acknowledgment of Ban on Nonpartisan Activities (c3, c4) (Spanish).....	196

Welcome

Introduction and Purpose

Over the last few years, prior to the 2016 election, we took 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. And in 2016 and now 2017 we have seen a marked rise in attacks, given the political context under which we work. 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 Molly Schultz Hafid of the Unitarian Universalist Veatch Program at Shelter Rock and members of the Neighborhood Funders Group, RoadMap, in 2012 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 initial “Getting and Keeping your House in Order” 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.

Please note that this toolkit is not for public distribution. It has been shared with clients and funders in a very targeted way, either connected to funding, services, or other direct arrangements with RoadMap. When distributing or reusing these materials with permission from RoadMap, please follow the Creative Commons guidelines below and attribute the materials to RoadMap and/or the original author.



This tool is free and can be adapted per creative commons guideline: RoadMap or the specific author.

Noncommercial use only, Share Alike (if you adapt or build on this work you can distribute under license identical to this one).

Acknowledgments

We are extremely grateful for funding from the following foundations that have underwritten WTS support for their grantees over the past five years:

- Unitarian Universalist Veatch Program at Shelter Rock
- Surdna Foundation
- General Service Foundation
- Public Welfare Foundation
- Solidago Foundation
- Hill Snowden Foundation
- The Ford Foundation
- Unbound Philanthropy
- Rosenberg Foundation
- The Discount Foundation
- Common Counsel Foundation
- Needmor Fund
- San Francisco Foundation
- East Bay Community Foundation
- Chorus Fund/Mott Philanthropic
- The California Endowment
- The James Irvine Foundation
- Borealis Philanthropy
- Ms Foundation
- Hyams Foundation
- Groundswell Fund
- Evelyn and Walter Hass, Jr. Fund
- Four Freedoms Fund/Neo Philanthropy
- LIFT Fund
- Training Resources for the Environmental Community
- State Infrastructure Project

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 during the creation and launch of WTS.

We would especially like to thank Molly Schultz Hafid of the Unitarian Universalist Veatch Program at Shelter Rock for all of her cheerleading, fundraising and unflagging support for this project! Ever since the need for a project like WTS was identified in 2012, Molly has been our primary guide and ally. Molly successfully helped raise money from peer funders for this project, contributed insight and knowledge to the creation of the webinar, toolkit, and technical assistance model, and continues to consistently remind the field that this work is critically important—and affordable, too.

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

The original 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](#).

The current Weathering the Storms team of RoadMap consultants and coaches includes Mary Ochs, Jennifer Soriano, Margi Clarke, Candice Cason, Amanda Berger, Scott Lowther, Mala Nagarajan, Lisa Jervis, Jonah Sheridan, Vega Subramaniam, Ejeris Dixon, Anbar Mahar, Monique Mehta, Mona Shah, Grace Kong, Suzanne Foster, Susan Wefald, Brigitte Rouson, Francisca Baxa, Jonathan Stribling-Uss, Pamela Chiang, Rusia Mohiuddin, Charles Fulwood, Janet McIntyre, and Hans Johnson. We also extend appreciation to RoadMap's Program Manager, Michelle Foy and Weathering the Storms Program Associate, Bev Tang.

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

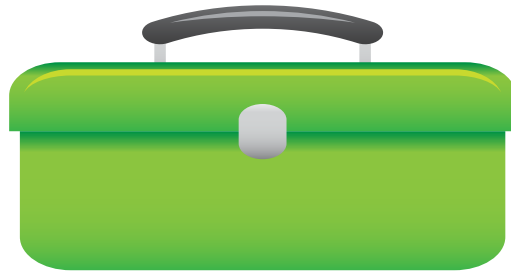
RoadMap is a national network of seasoned organizational development consultants dedicated to working with social justice organizations. RoadMap is the progeny of the successful Management Assistance Program (MAP) of the French American Charitable Trust (FACT) which conducted more than 70 organizational 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 60+ consultants and coaches have worked with over 110 additional organizations using a variety of capacity building modalities.

RoadMap's mission is to strengthen social justice organizations and the social justice sector through capacity building, peer learning and field building. RoadMap was established in 2011, and in addition to providing consulting services, RoadMap also serves as a forum for peer exchange and innovation, developing and testing new strategies to build healthy and sustainable social justice organizations, networks, coalitions and alliances.

RoadMap believes that in order to achieve transformational change, organizations and alliances need support to adapt to new challenges and changing conditions. RoadMap has taken a leading role nationally in providing this support through high-impact, relevant and integrated consulting, coaching, learning laboratories and other related services. Over the last five years, RoadMap has served over 110 social justice organizations and alliances through over 130 consulting projects.

Please learn more about us at www.roadmapconsulting.org. If you would like to Request Services or receive more information click [here](#) or send an email to info@roadmapconsulting.org.

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*
- 1.5 *Super Prepared Organization Sample Crisis Management Plan*

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.

Figure 1 - A Guide to Getting and Keeping your House in Order Checklist. Updated July 2017

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	<p>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).</p> <p>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.</p>	<p>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?"</p> <p>Helps keep organization aware of any potential issues of concern.</p>	
State and Local Registration and Reporting	<p>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.</p>	<p>Late filing of required reports & registrations makes your organization an easy target to be accused of operating "illegally."</p>	
Liability Insurance	<p>Insurance policy in place. Other specialized insurance coverage may be advisable depending on the nature of the organization's activities.</p>	<p>When holding events off-site, groups may need add-ons to their general liability policy.</p>	
Director and Officers Insurance	<p>Insurance policy in place.</p>	<p>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.</p>	
Workers Compensation Insurance	<p>Insurance policy in place and staff know how to respond in case of injuries or other claims.</p>	<p>Make sure employees are covered in all locations where they actually work.</p>	
Unemployment Insurance	<p>State requirement vary. Know your local, state and federal requirements regarding unemployment insurance. Most 501(c)(3) organizations are required to have this insurance.</p>		

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	<p>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.</p> <p>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.</p>		
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	<p>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.</p>	<p>Annual check in with an attorney regarding any changes in employment laws is recommended. A full legal review every 3-5 years is recommended.</p>	
Employment Forms	<p>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.</p>		
Independent Contractors	<p>Sign contracts and get W-9 from each independent contractor. File 1099 tax reports annually.</p>	<p>Ensure contractors are not doing work in ways that would make them employees.</p>	
Classification	<p>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.</p>	<p>Improper classification of temporary, seasonal, or part-time workers. Failure to pay minimum wage or overtime. Appropriate treatment of interns.</p>	

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. <i>(Note that this has some significant overlap with recommended policies for security readiness in Section 4 Digital Security Readiness Checklist under Item 4 on employee's responsibilities and limitations)</i>	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
Annual Communications Plan	<p>Organization should create an annual communications plan that advances organizational branding, mission and vision through all programs</p> <p>Your crisis communications plan will be integrated into this annual plan (see crisis comms section of toolkit)</p>	<p>Should be updated annually and include:</p> <ul style="list-style-type: none"> • Measurable goals achievable in one year • Specific audiences • Core messages 	
Comms Roles specified for Crisis Management Team (CMT)	CMT comprised of key staff and board members should have comms roles specified NOT just for comms people e.g.,: ED final-decision maker on comms strategy & spokesperson, Organizing Director develops issue-specific framing & messaging etc.	Contact information (i.e., cell phone numbers, email addresses, Signal contacts) should be frequently checked, updated, distributed to CMT members.	
Legal Counsel & Comms Support	Secure pro-bono or in-budget legal counsel and comms support through verbal or written agreement	If not pro-bono support, consider creating a defense fund so you have budget line item to pay for this additional support in case of crisis	
Trained Spokespeople & Third Party Validators	<p>Identify no more than 2 organizational spokespersons and train them in high-level spokesperson skills</p> <p>Create agreements with opinion leaders not directly affiliated with your organization who will vouch for your org reputation in case of crisis</p>	<p>Criteria to consider:</p> <ul style="list-style-type: none"> • Authoritative (e.g., CEO, President, Board Chair) • Credible (e.g. lawyer, accountant, public official) • Command of the facts • Able to speak without jargon • Able to emotionally Connect 	
Updated Media List	<p>Create and maintain a list of:</p> <ul style="list-style-type: none"> • Mainstream media makers • Media makers with issue expertise • Allied media • Your own grassroots media producers 	Update this list regularly – quarterly if possible, monthly is ideal	

8. Crisis Communications Planning		Risks to Watch For	Status at My Organization
Protocols for Internal & External Comms	<p>Create protocols for internal and external communications e.g.,:</p> <p>Internal protocols:</p> <ul style="list-style-type: none"> • Internal notification process • Secure communication during crisis • Online monitoring <p>External protocols:</p> <ul style="list-style-type: none"> • Social media protocol • Press protocol 	So that in case of crisis, you can respond quickly and effectively. Some protocols may actually help you prevent crisis.	
Crisis Communications Plan	Integrate a universal crisis communications strategy as well as threat scenario-based plans into your overall annual comms plan and overall crisis management plan (see crisis communications section)	The above protocols can become part of your universal crisis communications strategy. You can also create a crisis comms strategy and plans without an annual plan, but it may not be as effective in time of crisis.	

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 is 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 may 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

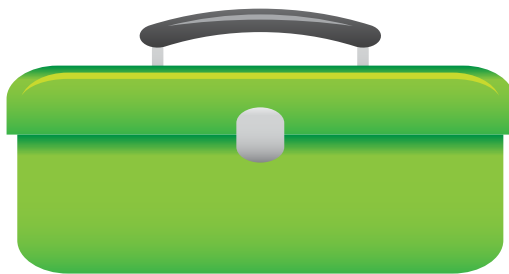
When the crisis has been resolved the CMT will meet to evaluate their management of the crisis and note lessons learned. The Crisis Plan may be adjusted based on the evaluation.

Figure 2 - Emergency Phone Tree

(updated May 1, 2017)

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 your 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)

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

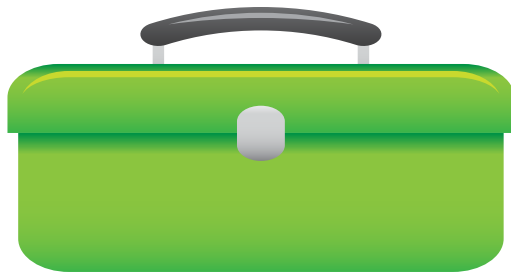
Any information on (ORGANIZATION'S NAME) electronic resources is the property of (ORGANIZATION'S NAME) and may be periodically reviewed. Employees have no expectation of privacy in connection with any information they store, send, receive, or access on (ORGANIZATION'S NAME)'s electronic resources. This 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 *Sample Compliance Calendar*
- 3.2 *Elements of a Crisis Management Plan*
- 3.3 *Sample Board of Directors Conflict of Interest Policy*
- 3.4 *Sample Whistleblower Protection Policy*
- 3.5 *Sample Document Retention and Destruction Checklist*
- 3.6 *Corporate Attacks—Limit Your Risks*
- 3.7 *Volunteer Screening and Protocols*
- 3.8 *Sample Intern and Volunteer Questionnaire*
- 3.9 *Sample of Volunteer Handbook Table of Contents*
- 3.10 *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 31 st (Sec State)
September	October	November	December
1 st dr 2018 budget			CT-2 to AG (fundraising) 31 st 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

(rev 7.6.17)

☐ Notification

At the first sign of an attack or potential attacks, the Crisis Management Team (CMT) should be notified immediately. Who is that team? _____. What are the best means for contacting them?

In certain types of emergencies your plan may instruct staff to first call 911 or alert law enforcement. Give very clear instructions in this regard. As part of creating you plan you will need to, in advance, your organizations policy on when and how to engage with law enforcement.

☐ Assess the Situation

- The CMT will assess the situation, determine facts, and begin delegating responsibilities.
- Line up specialty expertise in advance (ex. legal, communications, human resources, cyber specialists). Bring in as needed.

In advance of an actual attack it is important to determine what are the most likely types of attacks you are most concerned about.

Use this **risk assessment** to prepare some scenarios and your crisis communications plan. Practice your scenarios as part of training and internalizing you Crisis Management Plan

- Identify Likely Threats
 - Likely Adversaries?
 - What “assets” are affected?
 - Potential negative impacts?
- Assess impact level (high, medium, low level) & prioritize
- What protections need to be in place to prevent and prepare for these attacks?

☐ 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 handle

☐ 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.

☐ **Key Foundations, Allies and Members**

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

☐ **Message Platform**

Adapt your organizational message platform to address top threats

- Lead with org values and vision, and program demands when relevant
- Add talking points that address top threats and vulnerabilities
- Indicate what you will and won't say
- Develop accurate messages to discredit opposition

☐ **Communication Strategy**

Integrate a crisis communications strategy into your annual communications strategy

- Choose your top 3-5 threats, then for each:
- Identify objectives, audiences, frames and messages, talking points
- Document possible traditional and social media tactics
- Ensure your media lists are updated

☐ **Spokesperson Readiness**

- Identify no more than 2 organizational spokespeople, make agreements with third party validators
- Avoid too many spokespeople
- Train spokespeople on message discipline
- Practice away the top mistakes - "No Comment" or too many comments!

☐ **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 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 unless encrypted.

- Seek the advice of an attorney regarding document retention or destruction.

☐ **Post Crisis Evaluation**

- Evaluate the management of the crisis and lessons learned.

Engaging Law Enforcement

In advance of some emergencies or crises it key to know your policy on engaging with law enforcement.

Some members of your staff, board and your base/community may be uncomfortable with law enforcement presence or involvement.

-Be clear about when and how you wish to engage. What your organizational values are when engaging with law enforcement.

However, engagement with law enforcement is necessary if you want to file hate crime charges, if you have reason to need to file insurance claims or victim of violent crime claims.

When possible, build a relationship with law enforcement officials with whom you can build a working, respectful relationship.

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.)

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.

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

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 of 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 toINSERT 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 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
- ◇ Database 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:

objohnson.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 confidentiality 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

Harassment Bullying Sample Policy

Anti-Discrimination, Anti-Harassment/Bullying, and Affirmative Action

Discrimination Prohibited

[Insert organization name] does not discriminate unlawfully on the basis of perceived or actual race, color, religion, sex, gender, gender identity, national origin, ancestry, age, physical or mental disability, legally protected medical conditions including pregnancy and childbirth-family care status, veteran status, marital status, sexual orientation or identification, or any other basis protected by law.

[Organization name] prohibits discrimination against or harassment of any individual on any of the bases listed above. For information about the types of conduct that constitute harassment, please see the “Harassment” section below. This policy applies to all areas of employment, including recruitment, hiring, training, promotion, compensation, benefits, transfers. It is the responsibility of every supervisor and employee to conscientiously follow this policy. Any employee having any questions regarding this policy should contact their supervisor or the Executive Director. Any employee who witnessed and/or is subject to discrimination or harassment that violates this section should promptly contact a supervisor or the Executive Director. Any such employee may file a complaint as set forth in the “Problem Resolution” section of (Organization name) personnel policies and/or employee handbook.

Harassment Prohibited / Anti-Bullying Policy

[Organization name] is committed to providing a workplace free of sexual harassment, which includes but is not limited to harassment based on perceived or actual gender, gender identity, pregnancy, childbirth, or related medical conditions, as well as harassment based on such factors as race, color, creed, national origin, ancestry, age, physical disability, mental disability, medical condition, marital status, sexual orientation, family care or medical leave status, veteran status, or any other basis protected by law. [Organization name] strongly disapproves of and will not tolerate harassment of employees by supervisors or co-workers. Similarly, [Organization name] will not tolerate harassment by its employees of non-employees with whom [Organization name] employees have a professional relationship, this includes boards, volunteers, interns, vendors, and others. [Organization name] will also make diligent efforts to prevent and protect employees from harassment by non-employees in the workplace. [Organization name] is committed to preventing and ending discrimination and harassment even if the conduct has not risen to the level of a violation of law.

Harassment Defined

Harassment may take the form of verbal, physical, or visual conduct related to any of the legally protected bases described above. Such conduct constitutes harassment when: 1. Submission to the conduct is made either an explicit or implicit condition of employment; 2. Submission or rejection of the conduct is used as the basis for an employment decision; 3. The conduct interferes with an employee's work performance; or 4. The conduct creates an intimidating, hostile, or offensive work environment. Harassment may include, but is not limited to, the following: slurs, jokes, statements, or gestures; assaults; impeding or blocking another's movement or otherwise physically interfering with normal work; and pictures, drawings, or cartoons based upon an employee's protected status. Sexually harassing conduct in particular includes all of these prohibited actions as well as other unwelcome conduct, such as requests for sexual favors, conversation containing sexual comments, and other unwelcome sexual advances. Sexually harassing conduct can be by a person of any gender or sex, towards another person of any gender or sex.

Reporting and Investigating Harassment

[Organization name] understands that victims of harassment are often embarrassed or reluctant to report acts of harassment for fear of being blamed, concern about being retaliated against, or because it is difficult to discuss sexual matters openly with others. However, no employee or other persons should have to endure harassing conduct, and therefore, [Organization name] strongly encourages anyone to promptly report any incidents of harassment so that corrective action may be taken. Any incidents of harassment, including work-related harassment by [Organization name] personnel or any other person, should be reported to your supervisor, the executive director or to the Chairperson of the Board of Directors for investigation. Harassment complaints may be filed using the procedures described in the “Problem Resolution” section of this handbook or through any other formal or informal method. Any employee who receives a complaint or who observes harassing conduct should immediately inform a supervisor, the executive director or the Chair of the Board so that an investigation may be initiated. Every reported complaint of harassment will be investigated thoroughly and promptly and handled in as confidential a manner as possible consistent with a full, fair, and proper investigation.

It is important to create more than two independent channels of reporting, one that utilizes the usual levels of management and one that provides an anonymous channel to report harassment, discrimination, and potential whistleblower issues. Typically, the investigation will include the following steps: an interview of the employee who lodged the harassment complaint to obtain complete details regarding the alleged harassment; interviews of anyone who is alleged to have committed the acts of harassment to respond to the claims; and interview of any employees who may have witnessed, or who may have knowledge of, the alleged harassment. The Chair of the Board will notify the complainant of the results of the investigation. In addition to notifying [Organization name] about harassment or retaliation complaints, affected employees and others may also direct their complaints to the [Insert the State Agency that handles these complaints] which has the authority to conduct investigations of the facts. The deadline for filing complaints with the [State Agency] is *generally one year, but time may vary from state to state* from the date of the alleged unlawful conduct. If the [State Agency] believes that a complaint is valid, the [State Agency] may seek an administrative hearing before the [State Agency] or file a lawsuit in court. Both the [State Agency] and the courts have the authority to award monetary and non-monetary relief in meritorious cases. Employees can contact the nearest [State Agency] office or by checking the state government listings. The United States Equal Employment Commission (EEOC) has a time limit of 180 days to file complaints but may be extended by state laws.

Retaliation Prohibited

[Organization name] will not tolerate retaliation against any employee for making a good-faith complaint of harassment or for cooperating in an investigation. No adverse action will be taken against any individual for good-faith reporting of harassment. Retaliation by any [Organization name] employee against an individual reporting harassment is an unauthorized violation of [Organization name] policy, and will lead to disciplinary action.

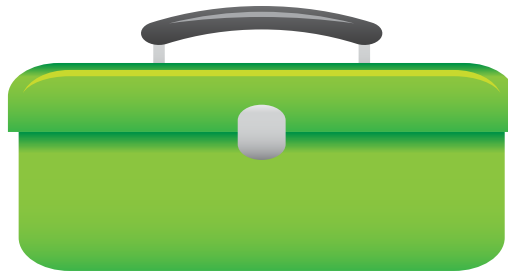
Corrective Action

If harassment or retaliation is established, [Organization name] will take corrective action that may include, for example: training, referral to counseling, or disciplinary action ranging from verbal or written warnings to termination of employment, or discontinuation of relationships, depending on the circumstances.

Harassment by External Stakeholders or Vendors

[Organization name] takes seriously any reports of harassment by external parties such as clients, vendors, funders, or contractors. Anyone in management who receives such a complaint should advise the Executive Director immediately. Management shall take immediate steps to de-escalate the situation, remove the offender, and safeguard all employees. In the case of workplace violence, call 911 or institute your community safety practices should your policy be to limit or not engage with law enforcement. Management shall work with the target of the harassment to identify next steps and to determine whether or not law enforcement should be contacted. Management shall investigate and take appropriate steps to address the situation depending on the severity of the offense. Steps may range from issuing a warning, cancelling service, getting a restraining order, and/or taking legal action.

Section 4: Digital & Data Security



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

4.1 Digital Security in a Nutshell

4.2 Digital Security Checklists Version 2.1

Public Wireless Use

Email Protection

Passwords and Authentication

4.4 Progressive Victory Scale of Organization Data Health

4.5 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 Version 2.1

Welcome!

You hold in your hands (or are viewing on your screen) a set of documents made to help US non-profits step into the work of securing their information and communications from the threats against it. At its heart is a group of checklists focused around a range of topics identified by consultants in the field that intentionally recommend constrained, accessible practices to help protect against widely available attacks on networks and devices. Adopting them will help you minimize security incidents - and the disruption and cost of viruses, malware, ransomware and phishing attempts. While these checklists can't fully protect you against powerful or persistent adversaries, the practices in them can make it harder for such enemies to attack your systems.

In addition to these lists of practices, this set contains a number of other tools and resources to help you succeed at implementing them:

- Immediately following this introduction, you will find [a tool](#) with instructions for assessing an organization's existing capacities and areas to develop in order to successfully take on this type of work. Completing this tool is recommended as a first step for all organizations.
- Directions and a legend explaining how to understand and use the checklists.
- The included glossary is meant to make digital security terms accessible to non-technical audiences and may be useful to print and share as part of training content.
- We have added a narrative Assumed Threat Model as an appendix to this document set for technical readers' reference. Recommendations are not annotated with specific threats mitigated at this time, but a technical support professional can help match assumed adversary capabilities with recommendations.
- An additional appendix of Frequently Asked Questions has been added with information on these checklists' origins and design.

About digital security

Digital security is a popular topic these days at conferences, in the media, and even around the dinner table. Yet in the deluge of information about nation-state actors, large scale attacks, and major vulnerabilities, taking action remains difficult for small organizations. Staff are often wondering, What does digital security even mean? And how can I get some it?

Really, digital security just means the set of practices used to manage the risk of bad things happening due to your organization's use of information and communications systems. That includes protecting them from being accessed, changed, or blocked by anyone or anything--internal or external, intentional or accidental--that shouldn't be able to do so. While we all spend a lot of time thinking about bad actors, sometimes the greatest risks are due to threats like fire or earthquakes.

The most effective security strategies, 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 face a shared set of baseline threats and vulnerabilities due to similarities in their operating conditions frequent reliance on the same systems and technologies. These documents are meant to help these organizations address the risks associated with these common needs as a first step in improving their security stances.

About organizational security

The adoption of new security practices always requires a **strong organizational commitment** as well as support from **organizational leadership**, because it changes the way you and your team work together. New tools and work flows are disruptive, even as they reduce your risk. It takes ongoing attention to turn policies and procedures into habits and to ensure that secure systems are regularly updated, working properly, and free of unexpected activity. The more you can build awareness about the particular threats your organization faces, the better you can select and commit to practices that will be useful for protecting your organization in its work. The more you can create a culture of learning and mutual support in your organization, the more success you will have in the uptake of secure tools.

In these checklists, we have identified solutions and practices across a range of levels of technical skill and organizational commitment that meet common threats that many, if not all, small organizations face. However, the effectiveness of these practices to protect from real threats is directly correlated with the investment you make in implementing them. Understand that there are always trade-offs associated with implementing new tools, and effort is required of staff to learn to perform tasks in new ways.

Treat digital security as the important organizational imperative it is by resourcing it appropriately and ensuring someone in your organization is responsible and has time in their workplan to manage digital security in an ongoing way. Take the time to identify your most sensitive information and communications in order to prioritize. Provide staff and volunteers the time, support, resources, and training needed to adopt any practices you undertake from these lists. In these ways, you ensure that the more you put in to securing your systems, the more you will lower your risk of bad outcomes.

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 Assessment Tool

Introduction

This assessment tool is meant to help organizations identify where their most critical security needs lie. Many common information systems and technology practices are oriented around providing or supporting security outcomes. Because of that, organizations that have foundational technology capacity issues are best served by putting energy improving baseline systems before taking on new security initiatives.

The tool is laid out as a number of items to assess broken out across three categories: cultural hallmarks of security success, information technology operations that support security outcomes, and digital security baseline capacities. Go through each section one by one.

For each item you, should grade your organization honestly on a scale from 1 to 10. At the end of each category, there is space to put a subtotal for that section.

After you have completed all three sections, add up the three subtotals to get your total score.

If you have a total score of 75, no section under 25 and no single item under 5 you should feel confident undertaking the rest of these checklists. Otherwise, your organization should concentrate first on any areas where you have very low scores, and overall on building capacity in these foundational areas before pursuing additional digital security improvements.

Even if you are at or above the thresholds indicated, be sure to note the places you have low individual or section scores and talk with your leadership and technology-responsible staff to make plans to improve them as soon as possible. Not consistently addressing and maintaining these foundational capacities will likely undermine your security efforts over time.

Cultural Hallmarks for Security Success

Score: ____ **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.

Score: ____ **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 is 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 offer licenses for their applications for free or at a discount, providing you significant capacity to centrally manage, back up, and monitor your information at a low cost.

Score: ____ **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 tools is a powerful modeling of preferred behavior and critical to changing organizational habits and culture.

Score: ____ **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.*

Score: ____ **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.*

Subtotal, Cultural Hallmarks: ____

Information Technology Operations that Support Security Outcomes

Score: ____ **Have a recurrent line item for technology in your budget.** *Security is an ongoing process and will require regular investments in computer equipment, software, support, and training to be effective. Work with your technical support provider to determine an appropriate amount to put into this line item.*

Score: ____ **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. Your tech support providers are central to your ability to identify and protect your systems from attack, work they can't do if they don't exist. There are as many ways to obtain technical support as there are organizations. Talking to peer organizations in your area is a good way to find quality help.*

Score: ____ **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 meet 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.

Score: ____ **Provide relatively new and adequately powered computers to all staff.**

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.

Subtotal, Technology Operations: ____

Digital Security Baseline Capacities

Score: ____ **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 to relevant organizational systems 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.*

Score: ____ **Make sure the computers and other devices you use, including personal devices that staff may use to access organizational information, are only running only the software expected, and only the most recent version of those programs. Have a plan to detect and remove malware, viruses, or other intrusive software and run update tools regularly.**

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 [TechSoup](http://techsoup.org) (<http://techsoup.org>). 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 Internet-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 (so you don't want them) but may also contain specific tools for the hardware, especially in laptops (so you may need them). Immediately after installation of the operating system and common software tools, run software updates for both the operating system and, where needed, the other software you have installed. Run these update tools regularly.

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.

Score: ____ **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 it seems expedient and can be cheaper to share accounts*

and login information, 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 G Suite or Office 365 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.

Score: ____ **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 at a minimum be 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 they were last tested. Refer to [Techsoup](http://www.techsoup.org/disaster-planning-and-recovery) (<http://www.techsoup.org/disaster-planning-and-recovery>) and/or [Community Innovators](http://www.communityit.com/resources/webinar-february-18-2016-backups-and-disaster-recovery-for-nonprofits/) (<http://www.communityit.com/resources/webinar-february-18-2016-backups-and-disaster-recovery-for-nonprofits/>) for ideas on how to improve your disaster preparedness.

Subtotal, Baseline Capacities: ____

Total Score (add up all subtotals): ____

Directions and Legend

Directions for Use

Before using these checklists

The first item in the set is a Digital Security Readiness Assessment Tool. We recommend you use this tool to see how prepared your organization is to take on digital security upgrades.

Since many foundational technology management and operations tasks underlie digital security capacity, or are even digital security tasks themselves, this tool is broken out into three categories: cultural hallmarks of security success, information technology operations that support security outcomes, and digital security baseline capacities. Follow the directions for the tool itself to find out how prepared your organization is before proceeding.

If your level of preparation is low in any broad category, individual item, or overall, that is the place to begin building your digital security capacity. If you decide to move on to the checklists in the meantime, be aware that your outcomes may be limited by these organizational dynamics.




Consistent attention to and maintenance of these foundational capacities is necessary for success in digital security efforts, so be sure to have a plan to keep improving your organization in these areas.



How to use the checklists

Once your organization has the readiness needed to take on some new security practices, you should proceed to the checklists themselves. They are compiled around specific topical areas, namely device security, authentication, wireless networks, email, and, for those who use it, G Suite.

We recommend pursuing these checklists in the order they are presented in this set, except that if you are using a specific platform, tool, or technology with dedicated a checklist of its own (such as G Suite) in which case you should start there.

All 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 hard to manage (as indicated by the  icons), technically difficult (as indicated by the  icons) and disruptive (as indicated by the  icons) a given step might be to undertake. Be sure to pick practices that match the time and resources your organization has available.

Be especially aware of the  rating, as it indicates disruption--only take on the practices with multiple  icons if you have the space to spend time as an organization absorbing training overhead and work flow transformation.

Legend



This check mark icon flags places for you to record actions you have taken. Cross them off or circle them as you go.



This spiderweb icon represents the amount of technology management overhead required to implement the item, in terms of the attention of leadership and technology-responsible staff inside an organization. One-spiderweb items should be doable by most technology capable organizations that have achieved other basic technology competency. Items with two spiderwebs may require additional time carved out beyond what regular operations demand, as they possibly require some outside assistance and work flow shifts. Three spiderwebs will require significant organizational commitment of resources to manage the project of implementing the recommendation, for support of renewed work flows, and to interface with technical assistance. Items with four spiderwebs are only for organizations ready to take on advanced security practices, including a part-to-full-time dedicated project manager as well as the ongoing commitment of human and other resources needed for process management, technical configuration, training, and ongoing support.



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



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 practice to achieve work flow shifts is required. One-bolt items will be mostly innocuous and staff can be trained in a brief session. Two bolts mean the practice will require more training and can disrupt existing work flows. Three bolts signal that significant work flow shifts and training will be required to undertake the practice. Four bolts mean the task will disrupt work flow completely and is only for organizations where security is of far greater importance than efficiency or convenience.

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.

Device Security Checklist

Introduction

This checklist comes from the Weathering the Storms toolkit, which contains wraparound documentation including an introduction, frequently asked questions, and a glossary where you can look up any terms that are unfamiliar to you. This is a community-driven document set with the latest version always at <https://ecl.gy/sec-check>. We welcome your feedback via RoadMap, or our contact form at <https://iecoology.org/contact/>.

Securing your devices or "endpoints" (meaning that they are one end of all connections you make to a website, online service, or other person's device) is a cornerstone of digital security. In general, security trainers and practitioners--and the documents and manuals they use--operate from an assumption that your devices are secure from intrusion and not running any malicious software. This is important because anyone who can control your devices can see and control all the same information you can, and so any protections of that information as it travels across internal networks or the open Internet become irrelevant.

Unfortunately, in practice, it is not a reasonable assumption in the operating reality of many non-profits and activists that our devices are not compromised. Especially with the increased use of encryption technologies to secure communications and other sensitive information as it moves over the network, attacks on hardware in devices themselves and, more commonly, the software running on them has become a more attractive strategy for obtaining or altering data. These factors combined mean that putting time and effort into securing your devices is a critical task for securing your organization and ensuring that any further steps you take to improve your security are meaningful.

This checklist provides a number of practices that can help you protect your devices from being vulnerable to threats to the confidentiality, availability, or integrity of the information stored on them or on the networks they connect to. By educating your staff about the importance of device protection, training and supporting staff in implementing these practices, and making device security part of your organization's onboarding processes and technology policies, you can increase security for individual staff and the organization as a whole. Furthermore, you can better trust that any other secure systems or services your organization adopts are protecting you as expected.

The recommendations on this checklist:

- Are meant to be applicable to computers, mobile phones, and tablets except where otherwise indicated.
- Do not constitute a complete set of endpoint device protection activities and are especially ill-suited for protecting you from targeted attacks by well-resourced and persistent organizations or entities.
- Will not fully protect you from the consequences of losing physical control of your device, especially situations where a technically capable group has physical access to your device such as may happen at an international border, if you are arrested or detained, or if your device is stolen. If your threat model includes these sorts of concerns, contact a digital security professional to help you build systems that will remain resilient in your specific context.

Key

- ✓ Record actions
- 🏠 Implementation management overhead
- ✂ Technical skill level required
- ⚡ Work flow disruption for staff

General Device Security Tasks for Computers, Mobile Phones, and Tablets

✓ **Keep your devices in your control, always.**



The easiest way to attack someone's devices is to gain physical control of them. Consequently, the most important practice you can follow to protect them is to keep them in your control at all times. This means that you know where they are and can ensure that nobody is accessing them without your permission. When working in a public place, don't leave any device alone even for a couple of minutes. Always take your phone with you, and do the same for a laptop. If you have to leave a device someplace, ask someone you trust (not the stranger at the next table!) to supervise it for you to ensure nobody tries to log in or insert any devices into it. This can be inconvenient but ensures nobody can surreptitiously install software on or hardware in your device without your knowledge. Note: There is a difference between keeping a device safe from theft and in your control. For example, keeping your devices in your locked office building may keep them safe from theft but does leave them accessible to any cleaners who come after hours. Even a hotel room safe can be accessed by the hotel staff. It is impractical to keep your device on your person as all times. (Devices become quite unreliable after being taken into the shower.) So, you should focus on reasonable controls to prevent bad actors from having physical access to your devices. Keeping your device at your home if it is properly secured, or locked in a drawer at night, can provide you a level of security that will force your adversaries to take more extreme means in order to compromise your devices.

✓ **Run the updating tool for your operating system and applications whenever updates are available and/or set updates to run automatically.**



The operating system is the most basic software a device can run, and every other program or application depends on it. Operating systems are often tied to specific hardware; major examples include Microsoft Windows, Apple's OSX (for computers) and iOS (for iPhones and iPads), Android, ChromeOS (for Chromebooks), and Linux. Nearly every update for operating systems and/or software also include security fixes. When updates become public, the vulnerabilities that they address become known by any bad actors who are looking for ways to exploit other people's systems. From the moment an update is released, you are at increasing risk of a bad actor using the vulnerabilities in that update against you until the moment you install that update. Setting updates to run automatically will help, but you should still manually

start the update process if you learn of a specific security issue with any of your software. If you don't want to run updates automatically, you should run your update process promptly when alerted that updates are available. Note that you may need to restart your device for many updates to take effect, so allowing your device to restart after an update is required for the update to provide protection.

If you have specific software requirements or custom software created for your organization, automatic updates can cause work disruption, as some OS updates may be incompatible with existing software. Therefore, operationalizing this recommendation must be coordinated with your IT team or tech support provider.

✓ **Use built-in full disk encryption on your devices and shut them down when they are not in use or are at risk of loss.**



Full disk encryption means that the contents of a disk, usually the storage inside your device--which contains the operating system, programs you have installed, and your organizational data--are scrambled so that they cannot be easily accessed when the device is off. Without this feature, someone who steals your device, finds your lost device, or otherwise accesses your hardware can easily read your files and possibly impersonate you to your systems.

Although full disk encryption is enabled by default on some mobile devices, it must be manually set up on all laptop and desktop computers, and many phones and tablets. The full disk encryption feature is called BitLocker on Windows (setup instructions and [licensing requirements](https://en.wikipedia.org/wiki/BitLocker#Availability) (<https://en.wikipedia.org/wiki/BitLocker#Availability>) vary depending on Windows version and hardware details), Filevault on OSX (find this under System Preferences>Security & Privacy), and LUKS on Linux (setup instructions depend on your distribution). On mobile devices running Android 5.0 and later, you can turn on this feature in the Security section of Settings menu. On iOS 7 and earlier, you can turn this on in the Passcode section of the General settings. Chromebooks and devices running iOS 8 or later have full disk encryption enabled by default. For advanced users, an open source encryption tool called VeraCrypt can also provide full disk encryption to Windows, OSX, and Linux computers as well as offering other advanced features; it can be found at <https://www.veracrypt.fr/en/Home.html>.

This recommendation is not effective unless is it coupled with the practices described in the next item, regarding device authentication and locking, to make sure the encryption cannot be easily bypassed when the computer is running.

Full disk encryption provides protection only when your computer is turned off, or turned on but awaiting a password to start up. Once you have logged in, the computer has the secret key needed for decrypting your data in its memory (so you can work!) and so even with the screen locked there is some risk of someone obtaining access to the contents of your computer while it is running or even sleeping. However, in general, surmounting those controls is a highly technical attack and that risk shouldn't stop you from keeping your computer turned on or logged in when you need to work. It is, however, best to turn off your devices whenever your device will be away from you in a hostile environment.

It is important to know that full disk encryption requires your device to do complex math, so turning on this feature will use processing power and may even make the oldest devices (around 5 or more years old) unreasonably slow to use. Full disk encryption can also increase the risk of you losing access to some of your information if robust password- or PIN-management practices are not in place. A lost password or PIN as well as failure of the part of the disk where the

encryption keys are stored will generally mean you (as well as anyone else) cannot recover your data. Ensure that you use syncing services and/or have regular backups of your data to minimize the risk of data loss. (Note that it is also critical to secure any synced or backed up copies of your data and the servers they are stored on.) Full disk encryption can also be used on external hard drives or USB sticks you use for backups using the same built-in tools mentioned above or by using VeraCrypt.

✓ **Use a strong password/pass phrase or long PIN code on all your devices, set your devices to lock themselves after a short period, and manually lock any device if walking away from it. Be aware of your surroundings when entering your password or PIN to ensure no one is watching and your movements aren't being recorded on camera.**



Always set up a long (8 numbers or more) PIN code or complex password (longer than 12 characters and including a mix of two or three different types of characters (e.g., symbols, numbers, and both upper- and lowercase letters)) to log in to any device--computer, phone, or tablet. This ensures that a lost or stolen device is inaccessible through its screen and the hardware remains encrypted. Use the screen timeout feature of your device and require your password or PIN to wake it back up to ensure that your information and your accounts are protected even if the device is found while turned on. The shorter the screen timeout period, the shorter the amount of time your device is vulnerable--so choose as short a time as you can while still being able to do your work. If stepping away from a device, manually lock the screen. Nearly every computer operating system has a keyboard shortcut or other quick way to lock a device (look it up in the relevant documentation or ask your technical support provider). Be aware when entering a PIN or password in public spaces to be sure nobody malicious is watching and that your keystrokes are not being recorded on camera. For mobile devices, biometric unlocking mechanisms (for example, fingerprints or facial recognition), swipe patterns, and other locking mechanisms are becoming more common, and are generally easier to use than complex passwords and long PINs. However, they can be more easily bypassed by, for example, grabbing your wrist and forcing your thumb into the button, holding your phone up to your face, or looking at the pattern of skin oils on your screen to see a swipe pattern. For these reasons, they are not recommended. This may change as implementations improve.

✓ **Turn off the built-in file sharing functionality on your device.**



Although handy for sharing files with peers, the built-in file sharing functionality on your device is vulnerable to abuse or accidental information leakage, especially on simple networks like one finds in cafés or on airplanes, which don't provide host isolation (the lack of host isolation means that any device using the wireless can connect to any other device). It is preferable to set up alternate tools and practices for sharing files, such as a central file repository in your office or an Internet-based file service.

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. Also disable AirDrop on your computer by going to the Finder, and choosing AirDrop under the Go menu. When the window comes up, you will see the phrase "Allow me to be discovered by" with a dropdown menu for completion. Choose "No One" from this dropdown. On an iOS device, select "Receiving Off" in the Control Center's AirDrop settings. See [this article](https://support.microsoft.com/en-us/kb/307874) (<https://support.microsoft.com/en-us/kb/307874>) for turning off file sharing on a Windows computer.

Recognize that if you are currently using any built-in file sharing functionality to share files inside an office, doing this will disrupt current work practices.

✓ **Run antivirus, anti-malware, and ad-blocking software on your devices.**



Antivirus and anti-malware software are programs that scan all files coming in or going out for files that are known to infect, steal data from, or otherwise abuse your device or data without your consent. While these tools work only against software already created, identified, and added to the software's lists of what to scan for, a large proportion of intrusions rely on these well-known threats. However, these types of software by their very nature must have access to all of the files on your computer, and so can themselves be a vector of intrusion. For this reason, you are best off with software made by a well-known manufacturer and vetted by your technical support provider. Never trust "free" or "no-cost" software promising to scan for viruses and malware, especially those that appear in pop-up advertisements in your web browser or on your device, as they often carry viruses themselves. TechSoup offers low-cost [Symantec](http://www.techsoup.org/symantec-catalog) (<http://www.techsoup.org/symantec-catalog>) and [Bitdefender](http://www.techsoup.org/bitdefender) (<http://www.techsoup.org/bitdefender>) antivirus software to most non-profit organizations. Both are available for Mac, Windows and Linux devices, but Bitdefender is also available for Android as well.

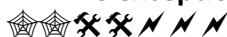
Note that the work of scanning for viruses and malware takes power from your device's processor, often a significant amount, so if it is already slow this may make your device unusable at times. Ad-blocking software will keep advertisements from loading on your web browser or device. Because of the complexity of modern ads, they can be vectors of attack, so you are safer blocking them entirely. Furthermore, removing advertisements should also improve your device's performance since it won't use your network connection to load, or use your processor to run, all of that often fancy (and insecure) content. However, ad-blocking software suffers from the same problems as antivirus software, and there are many that actually track you or inject other advertisements. uBlock Origin is a well-respected open source ad blocker that is available for Chrome, Firefox (including on Android), Safari, and Microsoft Edge. It can be downloaded from <https://github.com/gorhill/uBlock/>. **Note that there is another ad blocker called just uBlock or µBlock that uses a similar logo as uBlock origin but is not recommended.**

✓ **Install the HTTPS Everywhere extension on all of the web browsers you use.**



The "s" in HTTPS stands for "secure," and when you see "https://" rather than "http://" in your browser's address bar, it means that you are securely connected to the site you are visiting: The information being sent back and forth between your browser and the site's server is encrypted and so cannot be seen by others on the wireless network or the operator of the network itself. The browser extension HTTPS Everywhere forces your browser to connect using HTTPS instead of HTTP to any site that makes an HTTPS connection available, thus increasing the proportion of your traffic that cannot be viewed or altered by others on your network. You can install that plugin from <https://www.eff.org/HTTPS-EVERYWHERE>.

✓ **Be exceptionally careful about what software you install on your devices.**



The proliferation of mobile apps, browser extensions and other free (as in zero-cost, not open source) programs has caused numerous security problems. Avoid software that hasn't been created by a company you already have a trust relationship with (i.e., any company whose tools you are already using at your organization). Software that appears to have good intentions (like

antivirus scanning) or beneficial features may be masking malicious activities in the background. In most browsers and mobile devices, an application will ask for certain permissions at installation--the information and hardware it can access on your device. These are worth looking at to make sure they at least vaguely reflect what is expected. For example, if a flashlight app asks for permissions to your contacts or to make phone calls, you probably don't want to install it. Permissions to be especially cautious around granting include access to your calls, contacts, camera, microphone, location services, or entire storage.

The way to look at permissions after installation depends on the context. In Chrome, go to `chrome://extensions/` and click the permissions link for each one. On iOS devices, under Settings is a list of all permissions; under each permission is the list of apps that use it. On Android devices, go to Settings>Application Manager to view a list of apps; under each app is the list of permissions it uses.

Unfortunately, most software installation systems on laptops and desktop computers will not ask for permission to access resources, so you should be extra careful about installation of software not from a mobile, browser or OS app store.

Laptop and Desktop Computer Security Tasks

✓ **Add a privacy filter to your computer's screen.**



One of the easiest ways to accidentally leak information is for someone in a public place to see it on your screen. Purchasing and installing privacy filters (basically, a piece of plastic that allows what is on your computer to be seen only by the person sitting right in front of it), especially if you work frequently in libraries, cafés, co-working spaces, airports, and/or airplanes, will protect you from this threat. Be aware that if you frequently share information by showing your actual laptop screen to others (as opposed to by connecting your laptop to a projector or other display), you will want to ensure that any filter you purchase has an attachment option designed to enable easy temporary removal.

✓ **Carefully source your USB and memory card devices, only plugging trusted and personally sourced ones into your computer.**



Don't plug other people's USB devices and memory cards such as flash drives, hard drives, and phones into your computer, or any such devices that came to you in anything other than verifiable original packaging. This recommendation is especially important with regard to devices from unknown or untrusted sources (leaving USB sticks around an office is a classic intrusion technique), but it also applies devices owned by trusted people, as trusting a person is not the same as trusting all the devices they use, the software they run, or the other devices they have plugged their USB device into. USB and memory card devices can silently infect your computer in ways that are very hard to detect.

While never plugging USB devices into your computer is ideal, it is not always possible to do so. If you have to plug something into your computer, make sure that computer is running antivirus software that is up to date, and consider logging into a guest account that doesn't have access to your files or systems and then passing the files on it through an additional virus scan before opening or using. Certain Internet-based services, including Google Drive and Box (but not Dropbox) automatically scan uploaded files (under 25MB for Google Drive) for viruses and will

alert you if your files are infected, so you can use that as an additional layer of protection. However, there is still risk associated with USB devices and after using a USB device you don't trust, be on the lookout for odd behavior such as error messages, extra network traffic, or rapid battery usage and report any of those things to your technical support provider immediately.

Mobile Phone and Tablet Security Tasks

- ✓ **Don't click links sent to you by SMS or other text message, or through social media, especially from unknown parties.**



There is rarely a reason to send links in this way, and yet we continue to see situations where mobile devices are compromised through incoming links sent by text messages or social media messaging. Note this includes not just the common SMS text messaging that works on all cellular networks even without a data connection, but by also messages from any application that allows someone who knows your phone number or username to send you a message. The link may display what looks like a legitimate page, or often a shortened link, but may have installed malicious software in the background. If you absolutely need to click a link sent in this way, verify with the sender by phone or video call that the link you see is what they sent you. (Of course, this is broadly true of all links sent to you on all devices and over any channels that accept messages from anyone, for example, email or a comment form on a web page, so you should use caution in clicking those links as well.)

- ✓ **Use either a charge-only cable or what is known as a USB condom to charge your device from anything other than a wall charger or a computer that you know to be free of infection. Carry a backup battery to ensure you never have to charge your device from an untrusted source.**

Almost all modern professionals have been there: your mobile phone or tablet is dead and the only place to charge it a friend's laptop, an internet connected device, or a public computer. Unfortunately, that computer or device can become a route for a virus or other malicious software to infect your device. For use in these situations, you can purchase a USB condom (a device that goes in between the USB cable and the port you are plugging into and prevents a connection between the data pins in the unknown port and the USB cable, allowing only the power pins to connect) or charge-only USB cable (which does not contain the wires that are used for data transfer in the first place). Either option will enable you to safely connect your device to any USB port you come across. Another option, which has the added advantage of being useful even if you can't find a random port, is to purchase and carry a USB-enabled backup battery so you can always charge your device on the go. Although it has been shown to be possible, there have been no reports of backup batteries spreading malware. However, if charging from an unknown, you may want to use a USB condom or charge-only cable the way you would with an untrusted port to ensure that any software on the battery cannot affect your device.

Password and Authentication Safety Checklist

Introduction

This checklist comes from the Weathering the Storms toolkit, which contains wraparound documentation including an introduction, frequently asked questions, and a glossary where you can look up any terms that are unfamiliar to you. This is a community-driven document set with the latest version always at <https://ecl.gy/sec-check>. We welcome your feedback via RoadMap, or our contact form at <https://iecology.org/contact/>.

This checklist provides a number of 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 authentication (that is, proving your identity to a computer system), other systems are emerging that offer better protection. Some are mentioned below.

In the recommendations below, the term “organizational” is used to refer to the group of accounts that grant access to your organization's 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 what we are calling “everyday” credentials (the set of passwords that staff members need to perform their regular duties with databases, communication tools, and other platforms used for daily work).

Key

- ✓ Record actions
- 🕸 Implementation management overhead
- ✂ Technical skill level required
- ⚡ Work flow disruption for staff

Password and Authentication Security

✓ **Have all staff use password manager software.**



Since passwords can be used both to access organizational information and disrupt your work in various ways, they are one of the most important pieces of information to protect from exposure. They should never be stored in spreadsheets, text files, or word processing documents (even password-protected ones, as these are simple to break open); they should also not be saved to your browser's built-in password-saving feature.

Instead, use dedicated password manager software. This type of software will store all of your passwords securely and support you in adopting many of the practices listed in the items below. To use a password manager, you just remember a single password that opens up your secure file or account, which in turn stores all of your other passwords.

There are two types of password managers: those that are web-based and those that store information locally on your hard drive. Local storage is more secure, as web browsers are insecure environments for password storage and handling. KeePass and KeePassX are two versions of a highly recommended local password manager. These two tools use the same encrypted file format and can run on almost any computer. The excellent Security In a Box website has a [KeePass overview](https://securityinabox.org/en/guide/keepass/windows) (<https://securityinabox.org/en/guide/keepass/windows>).

We realize that web-based password managers (such as LastPass and 1Password) are efficient and appealing because they provide access to passwords where they are most often used: in a web browser. And although 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, the benefits do not outweigh the risks when storing rarely used core organizational passwords or other highly sensitive information. (See "Separate organizational and everyday passwords" below for more on this.)

✓ **Teach everyone in your organization to generate strong passwords and make sure they are used for all accounts, both organizational and every day.**



Strong passwords are generally 12 characters or longer and use a mix of two or three different types of characters (e.g., symbols, numbers, and both upper- and lowercase letters). Don't put uppercase letters, symbols, or digits specifically at only the beginning or end of your passwords; instead, mix them in throughout. Do not include any personal information like your favorite sports teams, places you have lived, your kids' or pets' names, important dates, or common phrases such as song lyrics or poems. Don't use patterns like "123" or "xyz," especially ones that appear on a keyboard, or acronyms associated with your work or organization.

There are many ways to generate strong passwords. There is a guide in [Security In a Box](https://securityinabox.org/en/guide/passwords) (<https://securityinabox.org/en/guide/passwords>), and most password managers will also make a random password for you, as will other available software for that specific purpose. [Diceware](http://world.std.com/~reinhold/diceware.html) (<http://world.std.com/~reinhold/diceware.html>) is a fun and effective scheme for creating random yet memorable passwords using everyday objects and a word list. One other great way to make a strong password is to come up with a silly sentence that no one's ever said before and use the first letter or two of each word as your password, mixing in other types of characters.

It is important to apply strong passwords to all accounts, as access to a single account can often be leveraged into access to other systems. This is especially relevant for any email accounts that can be used to reset or recover other passwords (usually via a "forgot password" link).

✓ **Don't use the same password for more than one site or service.**



Following this practice is a great way to minimize the risk of using third-party technology services. If you don't reuse passwords, someone learning your username and password for one service through a leak or break-in won't make it easy to access the other accounts you use. Use different passwords for each service so you aren't relying on the services you're logging into to protect your most important secret.

✓ **Try to limit hard-copy written password storage.**



Even when using a password manager, there are generally a few passwords you'll need to remember without it: the password to the password manager itself, of course, and probably at

least one device password. It can be tempting--and risky--to keep these written down on paper. Instead, use techniques found in the Security In a Box online guide listed above to create memorable but strong passwords. If you need a written copy of your password when you first start using it, protect it physically by storing it someplace where it won't be lost or stolen and easily identified with you. Try to type your password with less looking at the copy each time, and destroy the paper copy when you have memorized the password.

✓ **Do not tell anyone else your password(s), ever.**



Even if someone claims to be from IT or technical support, do not give them your password. Nearly every system allows for administrative reset of passwords for maintenance. Any legitimate IT person can use this function instead of asking you. This system also creates an auditable trail of access to your account, and alerts you to a reset. You will need to change your password again after such admin access, but taking that extra step will ensure that you and only you have access to your digital information, and that you can know who in your organization is responsible for what changes to your account.

✓ **Consider making single-use passwords for sites you rarely use.**



If you never store a password, you can never leak it and it can never get stolen from you. Most service providers allow you to reset a password by sending you an email. Creating and then immediately forgetting/not recording a long, random password is a good strategy when all of the following conditions are met: 1) The account is linked to an email address that you are sure you will control in the future, 2) the account is one you will not use frequently, and 3) you can absorb a potential delay in accessing the account if/when you need to.

When using this method, the next time you need to log in to the account, you can hit the "forgot password" link and go through the system's password reset process. Recognize that the security of any account for which you use this single-use method becomes the same as the security for your linked email account (since you use that email account to get back into the service) --so you need to ensure you have long-term access to that email account by ensuring that the domain remains registered in the long term and that the account password is strong and stored carefully.

✓ **Wherever available, and especially for critical accounts, implement two-factor authentication using a method other than text messaging as your second factor.**



Many service providers have begun to offer login systems that rely on more than one piece of information to identify a user, also called multi-factor authentication. There can be several items used for authentication, but usually there are just two: something you know (your password) and something else you have. In this case, we call it "two factor authentication" since there are two things, or "factors." Often the second factor is a code sent by text message to your phone (not recommended--see below), but it 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.

Two-factor authentication adds a layer of protection to your accounts so that it is much harder to take them over. It adds an extra step for people to get used to, but is a strong way to protect important accounts against weak or leaked passwords, as it protects from someone who obtains just the password from getting into the account. It is especially important to use two-factor authentication on accounts that grant a lot of access to your devices or files. Such accounts

include those that allow you to push software installs to devices (such as Apple IDs or Google Play accounts) or to reset passwords for other accounts (any account you use as a recovery email for other services, for example).

Be aware that cell phone-based authentication factors (whether via a text message or an app) require a working phone, so if adopting them you may wish to also provide staff with backup batteries to ensure they can always log in to their accounts even on days with heavy telephone use. In some cases, where login is only occasional, a piece of paper with preprinted backup codes may suffice, but then you need to protect that paper carefully.

A newer and very strong second factor is a code embedded on a special type of USB device also known as a "Universal 2nd Factor" (U2F) such as a the [Yubikey](https://www.yubico.com) (<https://www.yubico.com>). Not having a dependency on a working phone or cell signal is one of many advantages of U2F devices, but as of the latest update to this document in the fall of 2017, there are still relatively few services that support such U2F-capable devices. Major services your organization may use that support U2F keys include Dashlane, Dropbox, Facebook, Google, and Salesforce. You can read more about U2F at <https://www.yubico.com/solutions/fido-u2f/>.

Text message-based codes are not recommended for use as a second factor. It can be surprisingly easy for someone to take over control of a cell number via social engineering and/or fraud (see <https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief>, <https://techcrunch.com/2016/06/10/how-activist-deray-mckessons-twitter-account-was-hacked/>, and <https://threatpost.com/nist-recommends-sms-two-factor-authentication-deprecation/119507/> for more information). Adopt one of the other mechanisms above instead.

Access Now, an organization that "defends and extends the digital rights of users at risk around the world," has released a [clear and handy guide to choosing a two-factor authentication method](https://www.accessnow.org/cms/assets/uploads/2017/09/Choose-the-Best-MFA-for-you.png) (<https://www.accessnow.org/cms/assets/uploads/2017/09/Choose-the-Best-MFA-for-you.png>).

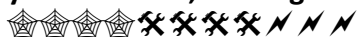
✓ **Separate organizational and everyday passwords.**



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.

Placing organizational passwords in a KeePass or otherwise encrypted 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 into your decision.

✓ **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 that people use strong passwords. It takes some advance planning and staff training, as setting up these controls without being clear on the implications can confuse users and 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. However, this step improves the security of all users at one time, so is highly recommended.

Wireless Network Safety Checklist

Introduction

This checklist comes from the Weathering the Storms toolkit, which contains wraparound documentation including an introduction, frequently asked questions, and a glossary where you can look up any terms that are unfamiliar to you. This is a community-driven document set with the latest version always at <https://ecl.gy/sec-check>. We welcome your feedback via RoadMap, or our contact form at <https://iecology.org/contact/>.

This checklist provides a number of practices that can help protect you and your staff when using wireless networks such as those in offices and co-work spaces as well as public places such as hotels, cafés, and airports. Because there are so many ways that wireless networks can be compromised, you should treat all wireless networks as having limited security. You are always safest directly wired into networks that you own and/or control.

If performing work using sensitive or confidential information, including anything that is 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 wireless networks for those tasks if possible and should never use a free or public wireless network for that work, unless you are using a VPN. (VPNs are covered below.)

Key

- ✓ Record actions
- ⚙️ Implementation management overhead
- ✂️ Technical skill level required
- ⚡ Work flow disruption for staff

Wireless Network Safety Tasks

✓ **Prefer Firefox or Chrome browsers. Only use Internet Explorer and Safari when required. Keep all web browser software, including extensions, updated to the latest version.**



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](https://google.com/chrome) (<https://google.com/chrome>) and [Firefox](https://getfirefox.com/) (<https://getfirefox.com/>) have led the development of this important feature.

✓ **Install the HTTPS Everywhere extension on all of the web browsers you use.**



The "s" in HTTPS stands for "secure," and when you see "https://" rather than "http://" in your browser's address bar, it means that you are securely connected to the site you are visiting: The information being sent back and forth between your browser and the site's server is encrypted and so cannot be seen by others on the network or the operator of the network itself. The browser extension HTTPS Everywhere, produced by the [Electronic Frontier Foundation](https://eff.org) (<https://eff.org>) forces your browser to connect using HTTPS instead of HTTP to any site that makes an HTTPS connection available, thus increasing the proportion of your traffic that cannot be viewed or altered by others on your network. You can install that plugin at <https://www.eff.org/HTTPS-EVERYWHERE>.

- ✓ **Install Privacy Badger, a browser add-on that will limit the "cookies" --small persistent chunks of information--set on your computer by websites.**



Privacy Badger (also produced by the [Electronic Frontier Foundation](https://eff.org) (<https://eff.org>)) is designed to help reduce the privacy breaches and tracking that come with the use of cookies. These cookies can be transferred insecurely and so can, if poorly implemented, expose login credentials or other information in transit. As an extra benefit, using this extension will increase your privacy and reduce the extent to which you are tracked online. Download it at <https://privacybadger.org>.

Note that if you are using integrations between different web-based systems in your work (for example, connecting file-sharing systems such as Google or Box to project management systems such as Asana or Basecamp), you will need to tune your Privacy Badger settings for those sites to keep the integrations working properly.

- ✓ **When you have a choice, pick wireless networks that use a password, ideally a unique one for each person connecting, and those that use WPA or WPA2 encryption rather than WEP encryption.**



A password on a wireless network means the information moving across it is less easily captured and decoded by someone nearby. However, in most cases everyone with that password can at least see some parts of your network connections--but if everyone has a unique password this becomes quite hard to do. WPA and WPA2 offer stronger protection than WEP, which is now relatively easily compromised. Most computers offer an easy way to view what encryption is in use on a given network. In OSX, hold down the Option key and click the wireless indicator in the top right corner to reveal extra information about each wireless network. The method for viewing these details is different in each version of Windows, so ask your tech support provider for assistance for the software you use. Note that some broad attacks on WPA encryption schemes have recently come to light. Consequently, this recommendation has only limited utility, and for sensitive operations a VPN or other encrypted connection is necessary to ensure the confidentiality of your information.

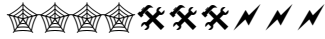
- ✓ **Confirm the network details before you connect.**



An attacker can set up an access point with a name similar or identical to a legitimate one, so that you connect to the attacker's network instead of the one 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.

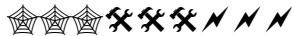
✓ **Ensure that the wireless network is not presenting false certificates, and do not import any certificates you are asked to install.**



Increasingly, networks are set up to monitor traffic for various reasons such as ad placement or content filtering. However, this potentially compromises all secure connections, as it allows traffic to be monitored via the same mechanism in what is called a man-in-the-middle (MITM) attack. Under these circumstances the network device will ask you to install a certificate that it controls and then will replace the security certificate from the service you are connecting to with the one you installed. Anyone with access to that device can now 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](http://patrol.psyced.org/) (<http://patrol.psyced.org/>), available only for Firefox, will help you identify certificate changes but in normal operation also causes many alert windows to appear as vendors change their certificates.

Google has created documentation for [viewing certificate information in Chrome](https://support.google.com/chrome/answer/95617?hl=en) (<https://support.google.com/chrome/answer/95617?hl=en>). Mozilla has [similar documentation for Firefox](https://support.mozilla.org/en-US/kb/secure-website-certificate) (<https://support.mozilla.org/en-US/kb/secure-website-certificate>) as well as some [overall instructions on connection security](https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure) (<https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure>).

✓ **Use a Virtual Private Network (VPN) to securely tunnel out of wireless networks.**



A VPN creates a secure connection for your computers and mobile devices to use to access the Internet (or an office network). This connection, or tunnel, can be used to hide all information moving between your computers and the Internet (or office network) from the operator or other users of the wireless network. Use of a VPN severely limits your exposure to the owner and operator of the network you are on and so significantly reduces the amount of trust you have to place in them. These factors make VPNs a very effective way to protect your traffic from observation or interception 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 hosts for you. If hosting your own VPN hardware, make sure you budget for ongoing maintenance, licensing, and software updates; otherwise, the device mediating your connection will become a vulnerability instead of a security improvement. Also recognize that in setting up a device to use for VPN connections inside your office, many offsite staff will be dependent on your office Internet line for their work. If this Internet connection is unstable, undersized, or asymmetric (made for downloading more than uploading, such as DSL or residential cable connections), the VPN will not work well for staff. For this reason, paying to locate your VPN device in a data center is the best way of getting a high trust, high-performance VPN in place.

Because of the high cost of self-hosted VPNs, most organizations choose to use a third-party VPN service provider to meet this need. This makes budgetary and operational sense; however, it is very important to vet a VPN provider carefully by thoroughly reviewing their policies, understanding their track record in the field, and checking client references. Recognize that unless you set up, run, and maintain your own VPN infrastructure, you are just offloading the trust you don't want to place in the operators of networks you are using to a different third

party--the owner and operator of the VPN service. While specific recommendations for VPN providers are outside of the scope of this document, in general, free VPN services, including those available in some app stores, should be avoided. (The adage "If you are not paying for it, you're not the customer--you're the product" holds true here.)

Choosing a provider of a VPN and setting up devices to use it are not simple tasks, and they are critically important--a misstep in setup or use can bring your work to a crawl or expose your information. All VPNs add a layer of network traffic and will slow down your Internet access, so your distance to and the bandwidth available from your VPN provider (or your office or data center if hosting your own) will make a difference to performance--and in turn whether people actually use it. The Electronic Frontier Foundation's Surveillance Self-Defense project contains [further information on choosing a VPN](https://ssd.eff.org/en/module/choosing-vpn-thats-right-you) (<https://ssd.eff.org/en/module/choosing-vpn-thats-right-you>).

Consider whether you can absorb the costs to make the speed and trust tradeoffs acceptable to you before choosing to implement a VPN. If you can, the investment in hardware, implementation, setup, and hassle is repaid by a solution that mitigates a range of threats associated with use of untrustworthy networks across many situations.

Email Safety Checklist

Introduction

This checklist comes from the Weathering the Storms toolkit, which contains wraparound documentation including an introduction, frequently asked questions, and a glossary where you can look up any terms that are unfamiliar to you. This is a community-driven document set with the latest version always at <https://ecl.gy/sec-check>. We welcome your feedback via RoadMap, or our contact form at <https://iecology.org/contact/>.

This checklist provides a number of practices that can help protect you and your staff when using email to communicate. Before sending 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 the emails you receive like a sealed 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 anything that is 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.

Key

- ✓ Record actions
- ⚙️ Implementation management overhead
- ✂️ Technical skill level required
- ⚡ Work flow disruption for staff

Email Safety Tasks

✓ **Train everyone in your organization not to send sensitive or controversial information over email whenever possible.**



Information in these categories include but are not limited to passwords, credit card information, Social Security numbers, health information, organizational strategy, and potentially damaging critiques or insults. Establish encrypted channels for sharing this information. Possibilities include a secure instant messenger, intranet site, internet-based file server, or even mailed USB sticks.

One readily available option is [Signal App](https://www.signal.org/) (<https://www.signal.org/>), which is used for end-to-end encrypted instant messaging and file sharing on mobile devices. There is also a [Signal extension for Chrome](https://chrome.google.com/webstore/detail/signal-private-messenger) (<https://chrome.google.com/webstore/detail/signal-private-messenger>)

that extends this functionality to desktops and laptops. As of September 2017, the desktop application is still in beta testing so not recommended for high-risk situations.

- ✓ **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 are generally 12 characters or longer and use a mix of two or three different types of characters (e.g., symbols, numbers, and both upper- and lowercase letters). 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 that you can complete with standard household items is called [Diceware](http://world.std.com/~reinhold/diceware.html) (<http://world.std.com/~reinhold/diceware.html>). See the [Password and Authentication Safety Checklist](#) in this document set for more recommendations in this area.

- ✓ **Establish an anti-phishing training and education program and give staff opportunities for practice through live testing.**



Phishing is when malicious 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. Be careful not to create a fear response rather than lasting motivation, focus on one or two elements to identify in each email, and try to be playful and emphasize/reward good practices rather than the negative experience of getting tricked. Never shame your staff for clicking on a bad link! (This episode of the podcast Reply All, ["What Kind of Idiot Gets Phished?"](https://gimletmedia.com/episode/97-what-kind-of-idiot-gets-phished/) (<https://gimletmedia.com/episode/97-what-kind-of-idiot-gets-phished/>), is an entertaining and insightful cautionary tale.)

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 “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 changes to settings. Suspicious emails or account behavior should be reported to a technical support person and you should preemptively change your password.

There are multiple companies that offer anti-phishing training and testing if you don't have internal capacity to provide it yourself. [Contact Information Ecology](https://iecology.org/contact) (<https://iecology.org/contact>) for referrals.

- ✓ **Always log in to email over a private connection.**



This means using an address that starts with <https://> for webmail, and turning on mandatory 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; however, it is not a justification to send sensitive information using email internally or externally.

✓ **Where you can, implement two-factor authentication for email accounts.**



Many email providers have begun to offer systems that rely on more than one piece of information to log in. 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. People will have to get used to having this extra step to log in to new devices, but it protects from someone who obtains either item from getting into the account. See the [Password and Authentication Safety Checklist](#) in this document set for more information on this.

✓ **Instead of sending attachments, store files on a server and send expiring links to the documents there.**



Email attachments present several risks, including their use as a mechanism for phishing. They are not protected from being viewed or altered between recipients, so you cannot ensure that the document you send is the same one that the recipient receives. A malicious server between you and the sender could replace it with any program or file they want, including a virus or malware. Additionally, file attachments tend to remain in recipients' email in-boxes, where they are harder to control. For example, if you filled out an order form using your organizational credit card, and emailed it to a vendor as a PDF, someone who breached their email account would have access to a document containing your credit card information for as long as it was not deleted from the server.

A better practice than email attachments 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. These links can be easily generated in almost all file-storage systems, whether they use servers in your office (such as a Windows file server) or on the web (such as Google Drive, Box, or Dropbox).

✓ **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, even if it appears to be from someone you know, check that it points to a domain name that you recognize and expect (such as [roadmapconsulting.org](#) or the domain where your organization's files are stored). In most email programs, as on the web, hovering over a link displays the URL it points to. If the link's destination is unexpected or unfamiliar, check with the sender to make sure the email is legitimate. Similarly, don't open an attachment unless you are expecting it and the file name is in line with that expectation.

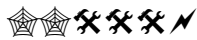
NEVER click on links or open files from unknown senders or in otherwise suspicious emails. Unlike people you know and are working with, someone you don't know will never send you a file that you actually need; if a link from an unknown sender actually contains useful information, you will be able to access it via another, more trusted method (for example, a web search).

- ✓ **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 IP addresses, accounts, or domain name marked, filtered, or blocked as a source of spam. You may also wish to send bulk email using a separate domain name from your main email (such as list.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.

- ✓ **Pay for a service to filter spam and viruses from email before it reaches your inbox.**



This service comes included with many email providers, including [Gmail](https://google.com/mail) (<https://google.com/mail>) and [Electric Embers](https://electricembers.coop) (<https://electricembers.coop>), but not all. 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 this may increase risk of that information being exposed. The [Electric Embers Cooperative](https://electricembers.coop/) (<https://electricembers.coop/>) is a values-aligned provider that offers such a service specifically for non-profits.

- ✓ **To prevent social engineering, use generic email addresses, and only those addresses, for critical functions such as finance, security, and human resources management. Forward critical staff's email to someone else rather than exposing their absence through out-of-office autoreplies.**



Social engineering is the psychological manipulation of people into performing desired actions, such as divulging confidential information or transferring funds. An increasingly common mechanism of attack on small business and non-profit finances is to look up the names of finance staff on the web and create fake emails to or from them requesting non-standard financial transactions due to some sort of emergency condition. Similar strategies can be used to obtain all sorts of information or to get people to take other types of actions.

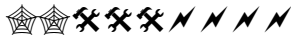
By using generic email addresses that don't contain staff names, you can help ensure these sorts of "person to person" social engineering attempts do not succeed, as it will make those attempts more obvious and less convincing.

Out-of-office autoreplies have also become a way for adversaries to gather intelligence about organizations, and identify periods when absences of key personnel may create opportunities to exploit lapses in standard operating procedures. Not exposing such absences by having email forwarded rather than automatically replied to reduces this risk.

All of these practices are strongest when coupled with strong internal controls for sensitive activities: standard, documented, and verifiable processes that require multiple steps involving multiple people for approval. For example, a typical internal control on transferring funds to

anyone requires a signature on a form and then a signature on a check or a wire transfer form for the bank. Instituting a practice of getting a voice confirmation from the executive director on any financial request outside of that process would prevent funds being stolen via social engineering.

- ✓ **Where email is accessed on mobile or laptop devices, configure email clients and web browsers to store as little information as possible.**



Most web browsers can and should be set to clear their caches 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. When set up this way, a lost or stolen laptop or phone will potentially result in far less exposure of information than it otherwise would. Note, however, that this practice will have extreme operational impact on your team, as it means that that users will need to enter a password every time they start their email program, and they will be unable to access emails when not connected to the Internet.

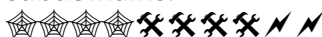
This practice can be made unnecessary by encrypting your devices' hard drives. See the [Device Security Checklist](#) in this document set for details.

- ✓ **Prevent targeted phishing attacks using look-alike domains by registering any domains that could be mistakenly read as the domain you use for your email.**



Phishing attacks are hardest to detect when they use email "from" addresses and links to websites that appear to be official but are actually hosted by the attacker. One way that this can be done is by registering domain names that look like other domain names--substituting a capital letter "I" for the letter "l," or an "m" for "nn," for example. For this reason, it is wise to note any ambiguous characters in your domain name(s) and proactively buy any that look similar. Although this will cost you some money, you can renew these at the same time as your other domains so there is little management overhead. You don't need to set up any services on these domains; you are just buying them so that others do not. [DNSTwister](https://dnstwister.report/) (<https://dnstwister.report/>) is a website that will let you put in a domain name and it will provide you a list of similar domain names that you might want to purchase.

- ✓ **Set up correct Domainkeys Identified Mail (DKIM) and Sender Policy Framework (SPF) records, and the associated Domain-based Message Authentication, Reporting & Conformance (DMARC) records that build upon these, for your email domains and subdomains.**



These are highly technical steps made in conjunction with your email and Domain Name Service (DNS) providers to make it hard for spammers or phishers to fake emails from your organization. Consult your technical support provider for help.

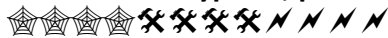
*SPF records identify which mail servers are permitted to send email on behalf of your domain. Be aware that setting this up requires identifying **all** the services that are currently sending email on your behalf (which could be databases, mass mailing tools, email list hosts, fundraising tools, and more); incorrect configurations can cause your email to be incorrectly marked as spam. Determining this list carefully is critical to implementing this recommendation in a way that does not interrupt ongoing operations. "Hard fail" settings (records ending in "-all") are preferred for SPF records wherever possible, but be careful, as this can cause email bounces if your records are not carefully tuned. Once set up correctly, however, you will need to maintain this list and make*

changes any time your organization adopts any other tools that send email from the same domain as your email addresses. Other than these maintenance steps, this should be invisible in operation. More information is on the [official SPF website](http://www.openspf.org/) (<http://www.openspf.org/>).

DKIM will help assure recipients that your designated mail servers sent the mail they are receiving. DMARC builds on these to tell recipient servers how to respond when the SPF or DKIM records help it identify spam or falsified messages. Once set up, these should have minimal impact on day to day operations, though it makes changing your email provider or infrastructure more complex. Find more information at the [official DKIM website](http://dkim.org/) (<http://dkim.org/>) and the [official DMARC website](https://dmarc.org/) (<https://dmarc.org/>).

Note that all three of these are easiest to set up using a platform such as G Suite, Office365, or other provider offering many services through an integrated, Internet-accessible platform.

✓ **Use encryption, preferably "end to end," to secure your email.**



This is a highly technical and labor-intensive initiative to undertake, but is probably the most complete way to minimize any inadvertent disclosure of data through email. Email encryption hides all email content from any servers or network providers that pass your mail along. It will likely require inconvenience for your team and significant changes to staff practices, but it provides strong protection of sensitive information emailed within your organization (and, if it is relevant to you, far greater compliance with standards such as HIPAA). There are various ways to implement email encryption, but only some are truly "end to end," meaning that you don't have to trust any parties in the middle, and encryption and decryption only happens on the devices communicating with each other.

The most common type of end-to-end encryption is called Pretty Good Privacy (PGP) and has been around for a long time. Consequently, there are a lot of ways to use this type of encryption, and it works across many platforms. (It also lacks the ease and strength of some other, more modern encryption schemes.) One major tool for using PGP encryption with email is the [Mozilla Thunderbird email client](https://www.mozilla.org/en-US/thunderbird/) (<https://www.mozilla.org/en-US/thunderbird/>) and the associated [Enigmail plugin](https://www.enigmail.net/home/index.php) (<https://www.enigmail.net/home/index.php>), which works on Windows (with the addition of [GPG4Win](https://gpg4win.org/) (<https://gpg4win.org/>), Mac, and Linux). You can find a guide for the Windows setup at <https://securityinabox.org/en/guide/thunderbird/windows>. OSX's built-in Mail program and the open-source add on [GPGTools](https://gpgtools.org/) (https://gpgtools.org) is also a workable toolset for using PGP-encrypted email on Macs. Microsoft Outlook works best with a commercial add-on called [gpg4o](https://www.giepa.de/products/gpg4o/?lang=en) (<https://www.giepa.de/products/gpg4o/?lang=en>) to use PGP encryption with Microsoft Exchange. [Mailvelope](https://www.mailvelope.com) (<https://www.mailvelope.com>) is a powerful and well-audited PGP add-on for web browsers that allows you to use PGP encryption with almost any webmail service, including Gmail. Because of its position inside a web browser, its security is generally less assured than the other PGP options above, but is adequate for many organizations, especially when coupled with strong web browser profile controls and careful use of browser extensions as well as other safe browsing practices. Note that as of mid-2017, use of Mailvelope in Firefox is not recommended due to a security vulnerability discovered in it. If you want to use Mailvelope with Firefox, see [this blog post](https://www.mailvelope.com/en/blog/security-warning-mailvelope-in-firefox) (<https://www.mailvelope.com/en/blog/security-warning-mailvelope-in-firefox>) for details of how to do so as safely as possible.

For organizations with more resources, S/MIME is an alternate encryption scheme that works well with a Microsoft Exchange/Outlook environment or with Gmail by installing the [Penango plug-in](https://www.penango.com) (<https://www.penango.com>) or using [Google's native offering](#)

(<https://support.google.com/a/answer/6374496>), which requires use of the G Suite Enterprise paid services.

As alternatives, several third-party-managed encryption tools for email exist. One popular such service is [Virtru](https://virtru.com) (<https://virtru.com>); it is available for Gmail and works best if used only with Gmail users. If you are able to transition your email entirely to their platform, [ProtonMail](https://protonmail.com/) (<https://protonmail.com/>) is an open source end-to-end encrypted email provider that has implemented common PGP encryption in a package that is easier to use than the toolsets named above and solves a lot of key management problems to make secure email more seamless for users.

Google's S/MIME option, ProtonMail and Virtru are end-to-end encryption offerings that function with a strong trust dependency on the vendor to produce, manage, and swap encryption keys for seamless emailing. If you are interested in these solutions, be aware that you are entering into a high-trust relationship with the vendor. If wanting to implement any encryption scheme mentioned here for your email, you will need to talk to your technical support provider and be prepared to invest time and resources into planning, implementation, and training.

G Suite Security Checklist

Introduction

This checklist comes from the Weathering the Storms toolkit, which contains wraparound documentation including an introduction, frequently asked questions, and a glossary where you can look up any terms that are unfamiliar to you. This is a community-driven document set with the latest version always at <https://ecl.gy/sec-check>. We welcome your feedback via RoadMap, or our contact form at <https://iecology.org/contact/>.

As of this document's creation (in 2017) a significant portion of U.S. non-profits rely on Google's free online applications (Gmail, Google Docs/Sheets, GDrive, and Google Calendar among them) to do their work. While many staff access these services through individual Gmail accounts (any username that ends with @gmail.com), or a link between their work email address and an existing individual account, Google also offers G Suite: a version of these tools suited for use in organizations. G Suite provides significant advantages over individual accounts, including organizational email addresses using your chosen domain name (the part of an email address after the @ sign), administrative controls, advanced settings, 24/7 tech support for use of the tools. These features can improve your organization's technology in many areas, including helping you better secure your information by providing tighter management, control, and monitoring of your systems and how they are used.

Because of these advantages, and the fact that Google offers the Basic version of G Suite for free to registered U.S. 501c3 organizations, setting it up for your organization is highly recommended for all eligible organizations that already rely on Google's web-based tools. While there are definitely risks associated with providing any third-party corporation access to all your information and the metadata about how and where you and your team use it--especially a corporation in the business of data mining and advertisement targeting--if you are already accepting this risk by relying on Google's tools, G Suite will at least help you secure that information from others. You can begin the sign-up process and read about the offerings at <https://www.google.com/nonprofits/products/apps-for-nonprofits.html>.

Please note that this document should in no way be read as an explicit endorsement of G Suite or other Google tools for movement-building, activist, or other non-profit organizations. There are many other tools--with a range of associated security and operational tradeoffs--that can meet the needs that G Suite fills. If any previous security risk assessment has shown that the vulnerabilities and risks associated with Google's tools are unacceptable for your organization, or if for any reason having strong trust relationship with a U.S.-based corporation is concerning to you, this checklist is not relevant to you and it is not a recommendation to rethink your existing decisions.

For those in the non-profit sector that have already adopted G Suite, the checklist that follows offers direction on how to set up and use the administrative controls offered by the free G Suite Basic platform to harden your organizational G Suite account and improve your overall digital security level. (In this context, "harden" means to reduce the points of vulnerability of a system by turning off or disabling functionality that is not needed.) Note that, as indicated in the associated descriptions, many of these tasks are specific implementations of checklist items from elsewhere in this set.

Please also note that there are additional controls and security features available using other editions of G Suite, including G Suite for Business and G Suite Enterprise. While neither of these

other editions are provided for free (and for a system that is priced by the user, costs can add up quickly), the additional functionality provided has tremendous value for organizations that have additional security needs stemming from items including but not limited to compliance requirements, the presence of highly sensitive data, or a wish to deploy tightly controlled mobile devices. You can review edition differences at <https://gsuite.google.com/compare-editions/>; if you're unsure which is best for your needs, ask for help from your technical support provider.

Key

- ✓ Record actions
- 🏠 Implementation management overhead
- ✂️ Technical skill level required
- ⚡ Work flow disruption for staff

G Suite Configuration Security Tasks

- ✓ **Make a plan, preferably before deploying G Suite, detailing how your information is used by your staff, volunteers, and others, to ensure that you understand your security needs and can configure the tools correctly.**



G Suite is a powerful platform with a lot of moving parts and a lot of possible configurations. As with all tools, the more time and energy you put into understanding the different users and user types you have and what features they need to use, the more effective your implementation of security controls will be. First read through this checklist to familiarize yourself with some practices you may want to employ in your G Suite setup. Then make a list of all the different groups of people you have in your organization that will be using G Suite; a typical list might be: full-time staff, part-time staff, volunteers, and board members. Then think about and list how each of those groups will need each of the various tools that are part of G Suite: e.g., to send email, to edit documents, to access your shared contacts list, to maintain a shared calendar, and so on. Does any single group need a tool that no one else needs? Conversely, does any group have no need for a tool that everyone else uses? Also think about any shared roles where multiple people need access to the same identity, email box, or set of documents -- such as an email account used to send or receive invoices, or a set of documents used for a volunteer-run hotline. Google has produced a lot of [documentation on how to plan your G Suite deployment](https://support.google.com/a/answer/4514329) (<https://support.google.com/a/answer/4514329>); reading through it will help you understand the applications and settings available to you in your configuration process. At a minimum, having a well-crafted plan will guide you as you step through the administrative tools at <https://admin.google.com> and also help you formulate specific questions for G Suite support as you go through the setup.

- ✓ **Create a single, dedicated account with full administrative control of G Suite ("Super Admin" permissions) and do not associate it with any individual's email address; provide a recovery email address or phone number that is controlled by your organization or a trusted tech support provider and not an individual employee. Assign other administrative permissions appropriately.**



While convenient, giving everyday user accounts permission to administer your G Suite creates risk. Doing so can mean that the loss or theft of a person's device, or a breach of their password, could put all of your organization's information at risk. Instead, sign up with or create a unique email address (like GSuite@yourdomain.org, replacing yourdomain.org with your organization's domain name) for this purpose; do not use it for anything else. Give this account "Super Admin" permissions (which means full control over your G Suite setup, including access to all calendars and accounts), remove those permissions from any other accounts (note that the account you use to perform your G Suite setup will have Super Admin permissions assigned automatically), and store the password in a safe way such as a well-configured password manager (see the [Password and Authentication Security checklist](#) for more information) or safety deposit box, using it only when you need to change settings in G Suite. You will be asked to give a recovery email or phone number in case of a lost password. This email or phone should be controlled by your organization or trusted delegate such as a tech support provider or affiliate organization rather than by an individual employee. You can find instructions for giving or taking away Super Admin permissions for a user at <https://support.google.com/a/answer/172176>. Directions for setting up a recovery phone number or email are at <https://support.google.com/accounts/answer/183723>.

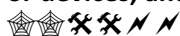
Other levels of administrative control can be assigned according to your organizational needs. For example, you could give a tech support provider Help Desk Admin permissions, which will allow them to reset passwords for people but not create users or groups. You can give control of that account to someone who does tech support without giving them total control of your systems. You can review the built-in administrative groups and find a link on how to make custom roles of your own at <https://support.google.com/a/answer/2405986>. Creating new users is the most common administrative task in many organizations and, although it may be tempting to delegate this permission to a normal operating account, gaining the power to create a user and add it to groups effectively gives a malicious actor access to all of your files until the user they create is identified and disabled, so it is best to give this permission only to specialized administrative accounts.

✓ **Enforce password length rules.**



G Suite allows you to set minimum (and maximum) password lengths. Setting a minimum length of at least 12 characters helps guard against easily guessable passwords. Instructions on getting this up are at <https://support.google.com/a/answer/139399?hl=en>. See the [Password and Authentication Security checklist](#) for more resources to help people create strong passwords.

✓ **Use the organizational units functionality in G Suite to make groupings of user accounts or devices, and give them the minimum level of access required to do their work.**



Giving all users ability to use all the G Suite tools in any way they want invites security risk for your organization. Instead, you should practice the security concept of "least authority"-- meaning you give users only the minimum access that is required for them to do their work. For example, you may want have volunteers enter information into Google Sheets but not send email from accounts with your domain name. To allow you to control access in this way efficiently rather than on a per-user basis, G Suite provides a structure called an organizational unit. Organizational units allow you to categorize users or devices into groups, and then assign policies to each of those groups. These policies cover things like the ability to access specific tools or to apply certain settings to their accounts. You can read an overview of applying policies at

<https://support.google.com/a/topic/1227584>. An article about organizational structures is at <https://support.google.com/a/answer/4352075> and instructions for creating units is at <https://support.google.com/a/answer/182537>.


Once you have created these units, you can use them to control access to services as described at <https://support.google.com/a/answer/182442> or to apply specific settings about those services as described at <https://support.google.com/a/answer/2655363>.

✓ **Use Google Groups and Team Drive features to provide appropriate access to files for different groups of users, and to ensure that your organization always controls its own information.**



Historically, one of the challenges of managing your organization's files using Google Drive has been the risk of loss of access to key documents when employees or volunteers leave the team, as well as the lack of ability to prevent sensitive information from being shared more widely than it should be. By setting up one or more Team Drives (as described at <https://support.google.com/a/answer/7212025>), you can ensure that the Super Admin for your G Suite domain always has access to the files that are stored there. You can also apply permissions (as described at <https://support.google.com/a/answer/7337635?hl=en>) to a Team Drive to allow only the minimum access needed. For example, you might have organizational policy documents that everyone needs to be able to view and only certain staff members should be able to change. You can give these permissions by individual email address if your organization is small enough, and, for larger groups and easier management, you can [create Google Groups](https://support.google.com/a/answer/33329) ((<https://support.google.com/a/answer/33329>)) and give appropriate permissions to the Group's email address. This way when a new person comes on board or leaves a team or the organization, you need only to take them out of the relevant Google Groups or Team Drives to also remove their account's permissions to files. Note that by locking down your files in this way, your system becomes much less widely accessible to staff, and someone will need to be in charge of and regularly available for changes to permissions and group settings as needed. The increased control of your files is well worth this overhead.

It is also useful to be aware that Team Drive permissions carries other operational tradeoffs around folder structure: it may limit who can create folders and move files around, which can benefit the clarity with which files are organized, but may also run counter to staff expectations and be quite disruptive. More expensive versions of G Suite also include Google Vault, which gives you a more robust set of tools for logging, archiving, and review of organizational documents for compliance or other reasons as described at <https://support.google.com/a/answer/2462365>.

✓ **Turn on two-factor authentication, and, in conjunction with appropriate planning, training, and support, enforce it for all users. Use Google Authenticator codes or universal two-factor (U2F) hardware keys as a second factor rather than text message codes, and make sure staff reports immediately if their second factor is lost or stolen.** 

One of the advantages of G Suite as a platform is its support for two-factor authentication, whereby users prove their identity at login with two things that they know or control: 1) a password and 2) a hardware key, code produced by a program running on their computer or phone, a text message code, a phone call to a cell or landline, or even a list or codes they have printed out. Unless your organization owns and manages the cell phones that would be receiving a text message or call, it is strongly advised that all staff use a second factor that does not rely on a text message or call to a cell phone when logging into Google services, especially for any

accounts with Super Admin or other administrative rights to your G Suite domain. This is because it can be surprisingly easy for someone to take over control of a cell number via social engineering and/or fraud (see <https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief>, <https://techcrunch.com/2016/06/10/how-activist-deray-mckessons-twitter-account-was-hacked/>, and <https://threatpost.com/nist-recommends-sms-two-factor-authentication-deprecation/119507/> for more information).

There are several alternatives to text messaging for this purpose. Google Authenticator is available in the Google Play store for Android phones, in the App Store for iOS devices, and as a Chrome extension for use in the browser. The most common U2F hardware key is called a Yubikey and can be ordered at: <https://www.yubico.com/gafw/>. Using this link and logging into your G Suite admin account will allow you to order up to 50 keys at the half-price cost of \$9 each.

Because of the choices available, the impact of this change on staff members' daily work, and the consequences of disrupted access to G Suite accounts, careful planning for the rollout of two-factor authentication is essential. Furthermore, enforcing two-factor authentication for all users requires each staff member to participate in this rollout in very specific ways. Refer to all the information and resources below to understand the scope of necessary planning.

Information about setup, as well as links to training materials for staff, is detailed in this document: <https://support.google.com/a/answer/175197>. Have staff print backup codes (see directions: <https://support.google.com/accounts/answer/1187538> so that they can still get into their account if their phone or hardware key is lost or stolen. Although those backup codes will allow them keep working, it is important to train users to report a lost second factor or set of backup codes to whoever is responsible for administration of your G Suite domain. Once reported lost or stolen, a security key **must** be revoked (<https://support.google.com/a/answer/2537800#seckey>), backup codes **must** be regenerated by the user (<https://support.google.com/accounts/answer/1187538>), or a Google Authenticator app **must** be removed as a second factor to preserve your security levels. Be aware that separate passwords for applications such as email or calendaring clients that do not support the two-factor process will become necessary, and you will want to be sure you help staff create those as outlined in this document: <https://support.google.com/a/answer/1032419>.

You can also use the Advanced Security Settings, which can be applied to all of your users, or any group of users in an organizational unit, to require that two-factor authentication is set up within a certain amount of time after a user's first login. Although this may put a strain on technical support resources, it is highly recommended. Directions to enforce two-factor authentication can be found at <https://support.google.com/a/answer/2548882>.

Note: A more general version of this recommendation can be found in the [Password and Authentication Safety Checklist](#) in this document set. Two-factor authentication is a best practice for use with any service or tool that supports it, and each will have its own set of options available--and planning steps--for you and your staff to consider.

✓ **Implement controls that make it difficult for anyone to spoof email from your domain.**



Google has produced a strong set of tools to allow other email systems to verify that email coming from your G Suite domain is in fact yours, preventing spoofed emails. (Email spoofing is the creation of email with a forged "from" address, generally sent with the intent to deceive the recipient.) Using them will make it very hard for your email addresses to be abused for phishing

or other attacks against external parties, as well as faked internally. These tools use the latest Internet standards called Domainkeys Identified Mail (DKIM), Sender Policy Framework (SPF) records, and the associated Domain-based Message Authentication, Reporting & Conformance (DMARC) records to do this. Documentation that will guide you through setting them all up is at <https://support.google.com/a/topic/4388154>.

Setting up DKIM, SPF, and DMARC is a highly technical set of tasks that involves your Domain Name Servers (DNS) in addition to Google. Your DNS may not be hosted at Google and so may require a different login; the management tools and may not have an easy interface to work within. It may be more appropriate to assign this set of tasks to your tech support provider than to do it yourself.

SPF records identify which mail servers are permitted to send email on behalf of your domain. Be aware that setting this up requires identifying **all** the services that are currently sending email on your behalf (which could be databases, mass mailing tools, email list hosts, fundraising tools, and more); incorrect configurations can cause your email to be incorrectly marked as spam. Determining this list carefully is critical to implementing this recommendation in a way that does not interrupt ongoing operations. "Hard fail" settings (records ending in "-all") are preferred for SPF records wherever possible, but be careful, as this can cause email bounces if your records are not carefully tuned. Once set up correctly, however, you will need to maintain this list and make changes any time your organization adopts any other tools that send email from the same domain as your email addresses. Other than these maintenance steps, this should be invisible in operation.

A more general version of this recommendation can be found in the [Email Safety Checklist](#) in this document set. It is more easily set up in G Suite than in many other environments, so here is rated slightly lower in difficulty and skill required.

✓ **Disable users' ability to set up automatic email forwarding on their account, so that any sensitive internal emails don't end up traveling insecurely to other email accounts or remain in less-secured email systems that are vulnerable to attack.**



Although it can be handy for people to be able to forward their organizational email automatically to personal or other email accounts, your organization has no control over how that email travels and how secured it is once it gets there. By allowing automatic email forwarding to other systems, you create a point of potential disclosure for internal conversations that would be otherwise locked into Google's secured infrastructure and (assuming you follow this checklist in full) protected by strong passwords and two-factor authentication. This is a simple setting that can be applied to all users or a set of users in an Organizational Unit as detailed at <https://support.google.com/a/answer/2491924>. Note this does not prevent a user from forwarding emails manually, emailing copy and pasted emails, screenshots, or downloaded copies of an email outside of your organization, so is best coupled with clear policies and guidelines in this area.

✓ **Change the default behavior of the "Get sharable link" feature.**

Unless you change the default behavior of your G Suite, whenever anyone clicks "Get sharable link" on a folder or file, they will create a link that is open to anyone, without needing to sign into a Google account. You can and should change this default behavior so that "Get sharable link" can be used to copy-paste a document link without changing the existing permissions on the item. Instructions for finding these settings are at <https://support.google.com/a/answer/60781?hl=en>; under Link Sharing, choose "OFF." This

setting will not prevent files and folders from being shared more widely by intentionally changing the item's permissions via the "Share" button.

✓ **Educate your staff on file sharing, including the higher security of sharing by email address and risks associated with sharing files by link.** 🌟🌟🌟🌟🌟

All users should be trained on the exact options available to them for sharing files in G Suite both with coworkers and external partners. This help document provides a good overview: <https://support.google.com/drive/answer/2494822>. Though this article is clear, helpful, and very suitable for end users, document sharing and collaboration work flows can be complex; it is recommended to document some guidelines based on your organization's specific ways of working and then offer in-person or webinar trainings, with live practice, to develop shared understanding and strong usage practices among staff.

The tightest control over sharing is exercised by clicking the "Share" button and filling out the "People" field with email addresses associated with Google-based accounts, whether inside your domain or not. When sharing in this way, you can copy the link from your address bar and share it safely, as it will remain accessible only to those with whom it has been shared. (Unless your G Suite's default behavior has been changed as detailed in the above item, clicking "Get sharable link" will change the permissions so that anyone with the link can view, without logging in.)

Situations will inevitably arise where a broadly accessible link is necessary (for example, if your external collaborator does not have a Google account or you want to cast a wide net for feedback). Be sure to consider the sensitivity of the document in these situations, and, when you choose to share this way, watch out for accidentally making a file public--be sure to choose "anyone with the link" instead. You should also train users to set an expiration date on shared links, even if it is far in the future. This will ensure that the file or folder in question eventually becomes unshared. Last but not least, it is important to choose the most limited permissions appropriate--allowing people who do not need to change its contents only to view and comment on a file.

✓ **Make sure someone is assigned to regularly monitor what is happening in G Suite, has time to do so, and knows how to identify and escalate any security incidents or other concerns about abnormal usage.** 🌟🌟🌟🌟🌟

Reporting on what is happening with your organizational tools and information over time is an important security practice. This is true for all tools, and an advantage of G Suite is that it makes this kind of reporting more accessible than in other tools. You want one individual or a team tasked with this ongoing monitoring, even if it's an external tech support provider, so that problems are caught quickly. Monitoring should be done on a schedule, no less than a monthly and preferably more often. To sustain this practice, it is essential that the person, team, or external provider is assigned this task via their workplan or scope of work. The goal of monitoring is to find unusual behavior, such as sudden growth in file sets or email activity, so the responsible party should first establish a baseline of normal activity and then look for trends outside of that baseline. Any questionable activity should be investigated with the users whose accounts are involved, or escalated to a tech support professional.


Activity Reports are available inside the administrative console, including use of two-factor authentication, external apps installed, emails sent/received, and file activity in Google Drive. An article describing these basic reports is at <https://support.google.com/a/answer/4580176>. A broader explanation of all the reporting available to you in G Suite can be found at <https://support.google.com/a/answer/6000239>.

In addition to this activity monitoring, it is important to regularly review the security settings of your users, especially password strength for any users not enrolled in two-factor authentication, as described here: <https://support.google.com/a/answer/2537800#password>. Google is continually updating their password-strength rating system in response to leaked passwords and other emerging threats, so a password that is judged strong one week may be judged weak the next. (This is less important for users with two-factor authentication, because in those cases as their password is only half of what is needed to access their account.) When you see a weak password in your systems, it should be changed. If you have regular contact with the user in question, walking them through changing to a better password is the best option. If you don't have regular access or they don't use the systems regularly, you can reset the password (using these directions: <https://support.google.com/a/answer/33319?hl=en>) so the account is protected, and communicate the new password to them via a secure channel; if you don't have a secure channel through which to give them their new password, you can reset the password and let them know that they should go through the "forgot password" process the next time they need to log in (be sure to follow up to make sure the new password they choose is strong enough). If appropriate to your operations and the frequency of their use of the account, you can also suspend the account and re-enable it as needed (<https://support.google.com/a/answer/33312?hl=en>).

- ✓ **Train users not to check the "Don't ask again on this computer" checkbox when using public or other untrusted computers, to logout after using such computers, and to untrust computers that are lost, stolen, or otherwise compromised.**



This practice will help ensure that all your other efforts to create high barriers to accessing your information are successful. When a user checks the "Don't ask again on this computer" box when logging into G Suite with two-factor authentication, they are telling Google not to ask for a password or second factor for 30 days. In the case of a poorly managed (i.e., not regularly cleaned or reset) computer in a library, Internet café, or other public place, this leaves an account wide open to abuse during that period. Though Google will prompt again for password changes and other sensitive actions, that computer retains the ability to access account information, send emails, and read and edit documents. Trusted computers can always be reviewed, and trust revoked, within a user's account settings as detailed here: <https://support.google.com/accounts/answer/2544838>.

- ✓ **Install Chrome on all staff computers and set it as the default web browser. Make sure staff know how to keep it updated and that they use Chrome instead of other browsers whenever they are using G Suite tools.** 

This practice will help you have strong security between your web browser and G Suite. Because Google controls both things, they have a lot of ways to verify that your connection is well-secured and that newer features like two-factor authentication work well; they can also push out corrected software if they have a security incident in their infrastructure. Generally, Chrome will self-update, but you should teach your staff how to recognize when an update is available (as described here: <https://support.google.com/chrome/answer/95414>). Quitting and reopening the browser will allow it to update to the latest, most secure version.

Appendix A: Digital Security Glossary

Add-on

See "extension."

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 with at least one up-to-date copy 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 set up.

Domain Name System

The domain name system (DNS) is like a phone book for the Internet. It translates domain names (such as ieco.org or reddit.com) 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

An encryption key is a piece of information that you share with an authorized party so they can encrypt and/or decrypt information to or from you. In most cases this information is highly sensitive and needs to be protected; however, some modern encryption schemes (asymmetric encryption, also known as public key encryption) allow you to have a public key that you can safely share with anyone.

Extension

A 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 a hardware device that sits between a device or network and the Internet. It analyzes and selectively blocks or alters information passing between two sides. 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.

Full disk encryption

An encryption setup where the entirety of a storage device, or disk--whether a USB stick, hard drive inside a computer or external drive for backups or any other--is encrypted. This is the most secure way of protecting your information as unencrypted parts of disks can accidentally hold sensitive data, even if just used for "virtual memory" or you think the files on it have been deleted. This is important especially for devices that could be lost, such as laptops, mobile phones, or backup drives--but will also mean that no data on them can be accessed (including for starting up the system in the case of a computer or phone) without the encryption password.

Office network

The equipment in your office that allows staff computers to connect to each other, 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.

Operating system

The main program that lets you run all the other programs on your computer. This usually includes all the tools to make your peripherals (such as keyboards or screens or storage devices) available and usually includes some sort of file manager--a way to find and access your files and programs. Common operating systems include Android, ChromeOS iOS, Linux, OSX, and Windows, but there are many others available used for all sorts of purposes.

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 systems.

Security certificate

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

Small Message Service (SMS)

Also known as a text message, SMS is generally an insecure way to send information to other people. It is relatively easy for those with technical equipment and knowhow to intercept cellular network traffic. In addition, many recent situations have shown that it is even easier to convince a cell company to hand over control of an account or to just steal a handset. SMS

should especially be avoided as a second factor for authentication (see "two-factor authentication" below) for these reasons.

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.

Two-factor or multifactor authentication

A way of identifying yourself to a computer or service that includes two or more items--often something you have (one-time code or specialized USB device) and something you know (like a password). Commonly one of those methods is an SMS message (see above); however, *this is no longer recommended and should be avoided due to the ease of gaining access to other people's cell service, phone, or SIM card.*

Virtual Private Network (VPN)

A connection between computers or devices that allows them to exchange information in an encrypted form. This can allow you to tunnel out of a network you don't trust or access information on your office network from someplace else on the Internet.

Wireless Access Point

A wireless access point (WAP) is 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 its more secure successor WPA2. Note, however, that some broad attacks on WPA2 have recently come to light as of October 2017.

Appendix B: Assumed Threat Model

Introduction

What follows is a simplified threat model that outlines the landscape in which these checklists are expected to be effective. You may note that many of these assumptions map to the individual items in the [readiness assessment tool](#), as they are foundational to the recommendations in the checklist.

These checklists do not promise to mitigate the threats listed here in their entirety. If all items in these checklists were to be implemented across an organization, any adversary as described by this threat model would face a high bar to impacting the confidentiality, integrity, or availability of that organizations' information systems. Although not annotated with this information, many single recommendations are directly oriented at defeating one or more of the listed adversary capabilities. If there is a specific capability that is of high risk for your organization, seek guidance from a technical support professional in determining which checklist items are most appropriate for mitigation of that risk.

We list the threat model in terms of assumed technical operating conditions, end-user skills, and adversary capabilities, delivered in narrative form rather than with technical detail. We believe this adversary profile fits both common criminal adversaries as well as low-skill political or otherwise aggressive opponents of non-profit organizations' work.

Assumed operating conditions

- Working environment is free from physical threat and devices are not consistently stolen or destroyed.
- Work is occurring primarily on adequately powered Windows or Mac computers with some use of Android or iOS phones for communications.
- All devices have been sourced through verifiable channels and are running official versions of operating systems.
- Devices do not cross international borders, though communications and data may.
- Work occurs using a limited set of applications and tools which are selected, administered, and managed by the organization.
- Authentication mechanisms for these systems may be open to login attempts from any device.
- Staff have regular and consistent access to the Internet to perform their work.
- Networks used to connect to the Internet may also be used by other organizations and the public—including potential adversaries.
- Networks in use do not also host publicly available servers or services.
- All organizational data is regularly backed up and available for restoration in a reasonable time period in most disaster circumstances.

Assumed end-user capabilities

- End users can physically protect their hardware and devices inside their homes and offices as well as when in public spaces.
- There is a mechanism for and end-user availability to provide/receive training in information systems topics.
- End users can operate the limited set of applications and tools their organization supplies for their use effectively.
- End users can install browser extensions on their devices. End users, technology-responsible staff or technical support providers can install other applications on end-user devices.
- End users can remember strings of letters, numbers, and symbols of length 12 or more for use as passphrases or shared secrets for accessing systems.

- Passphrases or shared secrets are used to authenticate a single or small group of individuals to a system.
- End users know how to request and receive technical support for problems with their information systems.
- End users know how to request files from backup repositories.

Adversary assumed capabilities

- Adversary can connect to publicly available information systems and attempt to authenticate with them.
- Adversary can send arbitrary content, including spoofed headers, malware executables, infected documents, and links to email addresses.
- Adversary can send arbitrary content to smartphones via SMS or other open messaging platforms.
- Adversary can use promiscuous mode on their networking devices to collect wireless network traffic from all networks.
- Adversary can use collected WEP encrypted wireless traffic to determine the password for that network and decrypt all content.
- Adversary can collect user credentials from unsecured exchanges on wireless networks with which they can authenticate or whose passive traffic they can otherwise decrypt.
- Adversary can set up wireless access points (WAP) in any public place with arbitrary or spoofed SSIDs.
- Adversary can use routing attacks to route traffic on public shared networks through their devices.
- Adversary can take over poorly configured or secured commodity gateway routing equipment using well-known credentials or attacks on out-of-date firmware sets.
- Adversary can spoof DHCP server announcements on public shared networks to attempt to act as the gateway for that network.
- Adversary with appropriate position (via routing/DHCP attacks, WAP spoofing, or router takeovers) can perform [man-in-the-middle \(MITM\) attacks](#) on unauthenticated traffic, including returning arbitrary results to DNS queries, downgrading STARTSSL email submission, rewriting unauthenticated exchanges, and sniffing credentials or other content.
- Adversary cannot generate or purchase certificates for arbitrary domains from commonly trusted Certificate Authorities (CAs) to MITM CA-mediated authenticated connections.
- Adversary can scan devices to identify their operating system or other software versions.

- Adversary can exploit well-known vulnerabilities in operating systems or local software with open listening ports.
- Adversary may be able to perform [evil maid attacks](#) on hardware that they have physical access to.
- Adversary may be able to use brute force mechanisms on hardware that they take possession of.
- Adversary cannot brute force encrypted information other than as noted in this document.

Appendix C: Frequently Asked Questions

Where did this document set come from?

This set of documents was made to help small non-profit organizations improve their digital security outcomes despite limited resources and technical skill availability. The content was commissioned as part of the [Weathering The Storms](#) initiative of [RoadMap Consulting](#), fiscally sponsored by [Common Counsel Foundation](#) of [Oakland, California](#). The content was researched and prepared by Jonah Silas Sheridan and Lisa Jervis, Principals of [Information Ecology](#), a capacity building consultancy specializing in non-profit and movement-building technology management, and was peer-reviewed by generous members of our community. Many other eyes and hands have helped tune the recommendations to ensure technical accuracy and ease of use. We are grateful to all the members of our community that have helped bring these documents to life.

When was this document set created and last updated?

This document was last updated in September 2017.

These documents were originally researched and peer reviewed in fall 2015. Some small edits and a minor 1.1 revision in spring 2017 updated and improved the [Readiness Assessment Tool](#) and other checklist language based on field experience. A major version 2.0 release was completed in September 2017. This version includes a review, update, and extension of the checklist set. It adds a [Device Security Checklist](#) and [G Suite Security Checklist](#), as well as an [Assumed Threat Model](#) for technical readers. All new content was peer reviewed. Contact [RoadMap Consulting](#) or [Information Ecology](#) with questions about this process or content.

If you have feedback or questions about this document set, its contents, or how to use it, please contact Information Ecology using [our secure contact form](#) or PGP encrypted email to info@iecology.org using [this key](#).

Why digital security checklists?

While computers have revolutionized and opened all sorts of new possibilities in how non-profits operate, 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 ways to manage them.

These checklists represent recommendations for a set of baseline digital security practices to help organizations move forward.

They have been created as a harm-reduction and capacity-building step to meet the common patterns in technical operations in small organizations. We have incorporated information from incident reports, emerging standards, current research, field experience, and community feedback about the work habits of and threats faced by non-profit organizations. The aim is to help organizations improve digital security outcomes by minimizing the easiest-to-exploit vulnerabilities in their systems. This strategy provides protection against many of the common attacks organizations are prey to while also helping create a stronger front against more advanced adversaries with time and resources to invest.

By minimizing the costs and disruption of routine security incidents (such as viruses, malware, ransomware, and phishing) and exposing staff to digital security topics and practices, it is hoped that going through these checklists helps create space for deeper risk analysis and organizational security

efforts. By stepping through these checklists, organizations can build their security practice muscles by implementing new, accessible habits and practices. Building this foundational capacity to tune operations is critical to taking on more advanced or disruptive security measures as the threat landscape changes.

What can't these checklists do for me?

The public-health concept of harm reduction is a useful approach to any situation for which a perfect solution is not available. Despite being an incomplete solution, regular hand washing is an important part of limiting the risk of getting certain illnesses. Similarly, a set of standard best practices represented by checklists cannot mitigate all risks, yet they can help protect you and your organization from some of the serious threats that come with using computers to manage your information. These checklists are meant as a starting point in understanding and responding to the most basic threats computer users face today. They are a useful first step to secure ourselves, our organizations, and our movements, but they are not sufficient. For those of us working in extremely hostile environments; aligned against highly repressive regimes; in closing political spaces; or in high-risk conflicts, disasters, or other unrest, a more rigorous approach is necessary. When significant risks of bodily harm, long-term detention, and death exist, these checklists cannot substitute for a more aggressive and thorough security analysis and response.

Effective security is an ongoing process. It requires consistent practices to be undertaken by all staff, 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 implementing new security practices puts pressure on key organizational processes and personnel. Implementing the checklist recommendations will generally not immediately make your work smoother and easier. Instead, many will likely create some disruption and training needs. In order to make meaningful strides in security, your organization must be prepared to make these trade-offs.

These investments in time and attention will repay the organization in smoother, more tightly defined operations--as well as peace of mind that come from knowing that those operations protect your data and systems.

Who are these checklists for?

Different and changing contexts, whether technical or geopolitical, introduce a variety of threats, vulnerabilities, and adversaries to consider in managing risk. To make these checklists useful, we have designed them to apply to a specific set of organizations and set of threats.

These checklists target organizations broadly seeking to protect themselves from security threats from non-persistent adversaries with limited resources (e.g., disgruntled individuals, identity thieves, political opponents, internal threats) rather than advanced persistent threats such as the U.S. government, other governments, or other large global entities including multinational corporations.

If your threat model includes advanced persistent threats, you will need to contact a digital security professional to help you build security practices and systems beyond those recommended in these

checklists in order to remain resilient in your specific context. [Contact RoadMap](#) or [Information Ecology](#) for help or referrals.

To keep recommendations actionable, we also made some assumptions about the operations of the organizations using these checklists.

- The organization has a staff of under 50 with an in-house technical team of no more than three, if any technical staff at all.
- The organization uses primarily desktop and laptop computers, with some use of mobile devices to access its information systems.
- The organization uses networks for work that are free from malicious outside interference and are segmented from the open Internet by a password-protected firewall device running up-to-date software, controlled by the owner.
- Although the organization may communicate with partners abroad, its staff neither cross international borders while carrying the organization's equipment or data, nor regularly work in a foreign country.
- The organization can in general successfully protect physical access to its office spaces, network equipment, and devices.

While these practices can certainly be adopted in environments that don't meet this profile, in those cases our rating system may not be accurate, and all recommendations should be reviewed by your technical or security support personnel.

Constitutional Communications Strategic Security Planning

By Jonathan Stribling-Uss

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.

Figure 24 - 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:	

Figure 25 - Compartmentalization Strategy

(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)

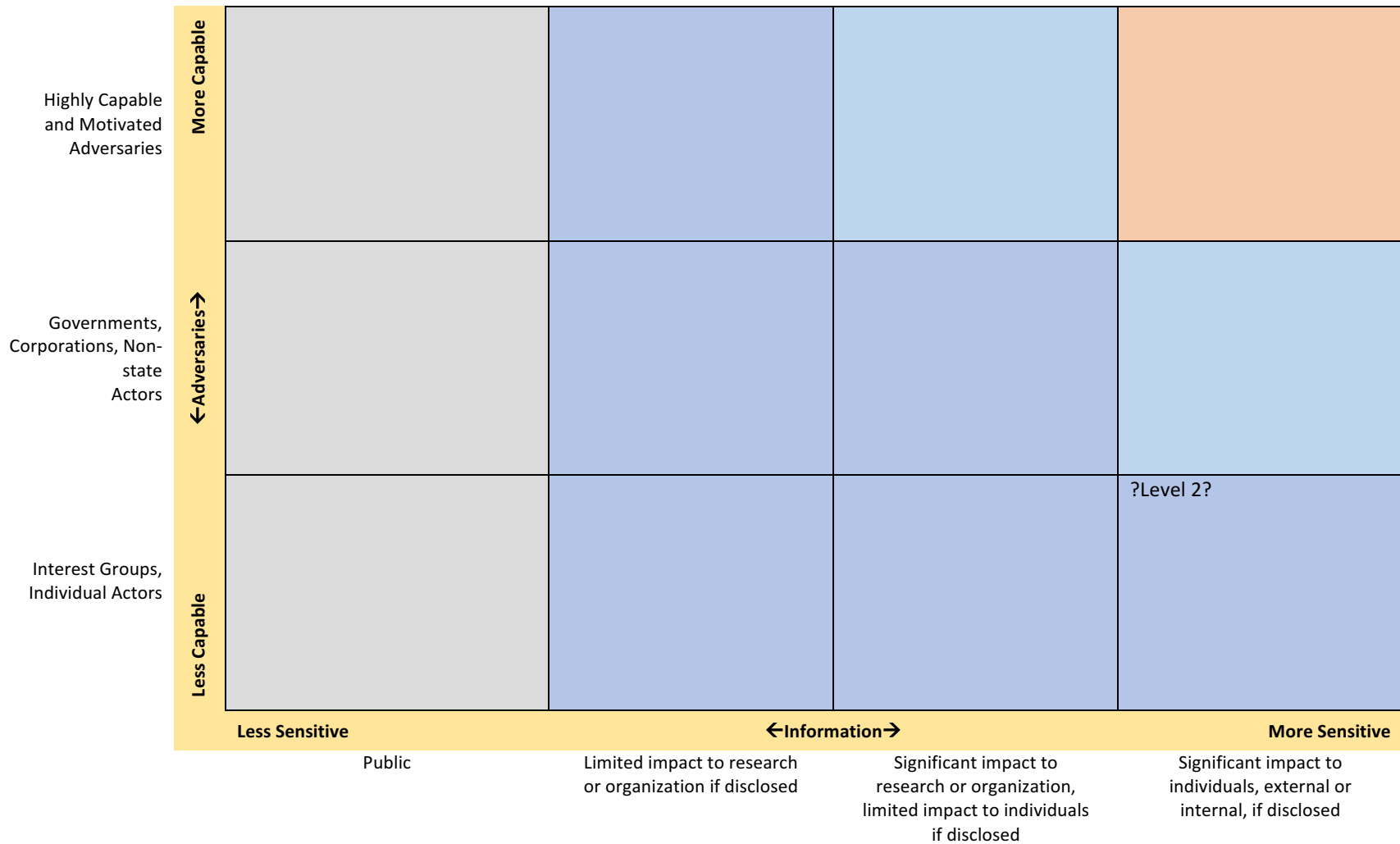


Figure 26 - Workflow Security Level

Changes in Workflow, in addition to basic security practices

Required <ul style="list-style-type: none"> • Signal message encryption • Full disk and device encryption • Only use organization-issued computer and phone (if part of a larger organization) 	Required <ul style="list-style-type: none"> • End-to-end encryption for all communications <ul style="list-style-type: none"> ○ 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 <ul style="list-style-type: none"> • Consultation with trusted security agents
Recommended <ul style="list-style-type: none"> • End-to-end encryption for all communications • Border crossing security 	Recommended <ul style="list-style-type: none"> • Consultation with trusted security agents 	Possibilities <ul style="list-style-type: none"> • Only work on computers disconnected from the internet • No communications that are not end-to-end encrypted • No closed systems for communications <ul style="list-style-type: none"> ○ No Skype, Whatsapp, telegram, etc.

Example Threat Matrix by Mala Nagarajan:

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
<i>Example: Physical attack</i>	<ul style="list-style-type: none"> • Staff may be injured, killed, kidnapped, traumatized • Non-injured staff traumatized • Operations stop • Time spent providing staff and community support 	<ul style="list-style-type: none"> • 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) 	<ul style="list-style-type: none"> • Staff • Office space and surrounding area • Physical files and computers 	<ul style="list-style-type: none"> • High security building • Secure communications process in place for crisis 	LOW	HIGH
<i>Example: Schmear campaign against org</i>	<ul style="list-style-type: none"> • Funders lose trust in organization • Allied orgs lose trust in organization • Research considered suspect • Time spent communicating with constituents to regain trust 	<ul style="list-style-type: none"> • Anti-X opposition • Elected officials supported by anti-X opposition 	<ul style="list-style-type: none"> • Org reputation • Staff reputation • Funder reputation • Ally org reputation 	<ul style="list-style-type: none"> • High security building • Secure communications process in place for crisis 	MED	HIGH

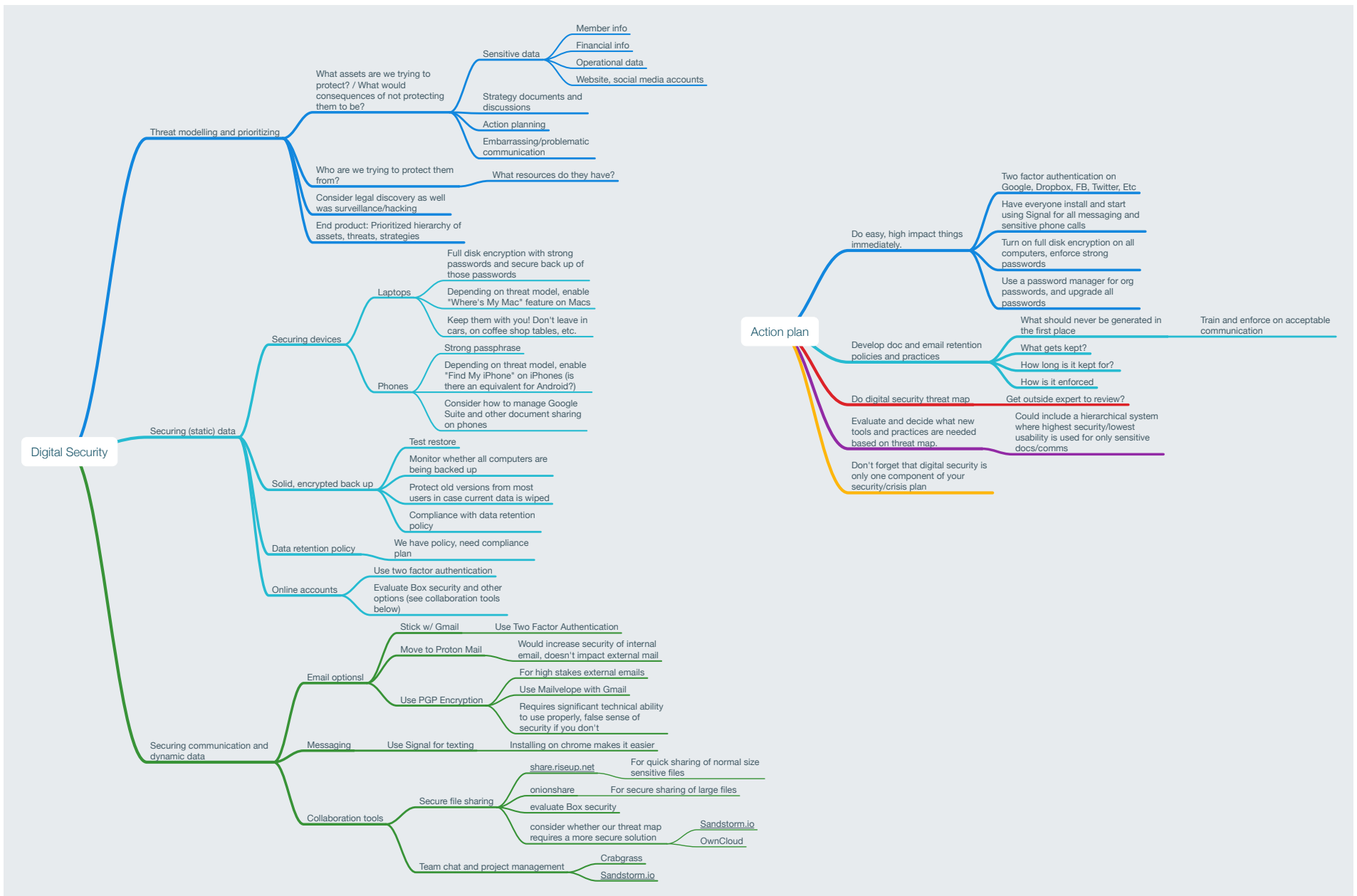
Threat	Potential Impacts	Adversaries (be specific as possible)	Assets Affected/ Involved (be specific)	Protections in Place (be specific)	Risk / Likelihood	IMPACT LEVEL
<i>Example: Email hacked</i>	<ul style="list-style-type: none"> • Emails sent in the name of organization • Personal information about staff are disclosed, leading to staff safety issues • Organization and staff are targeted with smear campaigns • Email exchanges between org staff or to external parties are taken out of context • Time spent communicating with constituents to regain trust 	<ul style="list-style-type: none"> • Anti-X opposition • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring) 	<ul style="list-style-type: none"> • Email server • Emails of individuals • Contact information stored through email client 	<ul style="list-style-type: none"> • High security building • Secure communications process in place for crisis 	HIGH	HIGH
<i>Example: Bank assets frozen</i>	<ul style="list-style-type: none"> • Unable to access money to pay staff and other expenses • Organization and staff are targeted with smear campaigns • Time spent investigating, recovering, resetting, and re-securing account • Time spent communicating with donors 	<ul style="list-style-type: none"> • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring) • Bank administration? 	<ul style="list-style-type: none"> • Money 	<ul style="list-style-type: none"> • 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
<i>Example: Financial theft / unauthorized</i>	<ul style="list-style-type: none"> • Money is stolen • Unauthorized charges • Time lost investigating, recovering, resetting, and re-securing accounts • Time spent communicating with donors 	<ul style="list-style-type: none"> • Anti-X opposition infiltrator 	<ul style="list-style-type: none"> • Money 	<ul style="list-style-type: none"> • Assets distributed across different banks • Cash on hand • Conversations with funders to enable access of emergency funds 	LOW	MED
<i>Example: Database (DB) hacked</i>	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Anti-X opposition • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring) 	<ul style="list-style-type: none"> • Contact information of clients, constituents, and collaborators 	<ul style="list-style-type: none"> • 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	
<i>Example: Social media hacked</i>	<ul style="list-style-type: none"> • Messages sent in the name of organization • Organization and staff are targeted with smear campaigns • Time spent investigating, recovering, resetting, and re-securing account; time lost communicating with constituents to regain trust 	<ul style="list-style-type: none"> • Anti-X opposition • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring) 	<ul style="list-style-type: none"> • Facebook • Twitter • ... 	<ul style="list-style-type: none"> • 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
<i>Example: Shared document repository</i>	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Anti-X opposition • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring) 	<ul style="list-style-type: none"> • Online storage (e.g., Dropbox, Box, Google Drive/Apps, Sharepoint) • Documents 	<ul style="list-style-type: none"> • 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
<i>Example: Devices stolen or confiscated</i>	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Anti-X opposition • Gov't officials (NSA, CIA, FBI) supported by anti-X opposition (under guise of security, monitoring) 	<ul style="list-style-type: none"> • Computers • Contact information stored locally • Phone call records, instant/chat messages • Works in progress 	<ul style="list-style-type: none"> • 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
<p>Compartment: PUBLIC</p> <p>Types of information: Public information, press releases, tweets</p> <p>Technical requirement: Twitter account, Facebook account, etc.</p>
<p>Compartment: DONORS</p> <p>Types of information: Donor contact information, non-publically available information</p> <p>Technical requirement:</p>
<p>Compartment: INTERNAL</p> <p>Types of information: Organizing strategy</p> <p>Technical requirement: Email, Signal, Jitsi.org</p>
<p>Compartment: STAFF</p> <p>Types of information: Personnel information</p> <p>Technical requirement:</p>
<p>Compartment: SECURITY</p> <p>Types of information: Crisis communications, passwords and social security numbers</p> <p>Technical requirement: Onionshare and signal</p>
<p>Compartment: TEXT/CHAT/SMS MESSAGING</p> <p>Types of information: emergency/private communications</p> <p>Technical requirement:</p>
<p>Compartment:</p> <p>Types of information:</p> <p>Technical requirement:</p>



Scale of Organization Data Health Tool

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.

© 2012 Progressive Victory. For more information about the PV ODH Scale, please write info@progressivevictory.com.

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.

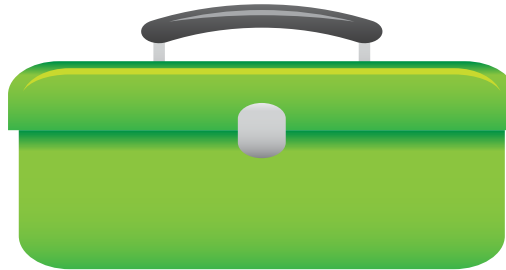
SPF records. Sender Policy Framework (SPF) is a system that allows you to tell others what servers and services are allowed to send email for your organization's domain name. Setting up this record requires the assistance of your DNS provider and can have unintended negative consequences for your email 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: Creating Community & Office Safety



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

5.1 *Office Security Series*

- De-escalation Methods and Tactics
- Tips on Creating Office Safety Protocols
- Entrapment Prevention and Preparation
- Creating a Community Security Plan for Actions, Events, and Demonstrations

Office Security Series: Entrapment Prevention and Preparation

Office Security and Safety Series

This document is part of RoadMap's Weathering the Storms--Office Security and Safety Series for social justice organizations, done in collaboration with Vision Change Win. The series seeks to equip organizations like yours with the resources and tools to manage different types of situations and/or crises your organization may face. This series currently includes several webinars and the following documents:

- De-escalation Methods and Tactics
 - Tips on Verbal De-escalation
- Tips on Creating Office Safety Protocols
 - Office Safety Sample Inventory
 - Office Safety Planning Worksheet
- Entrapment Prevention and Preparation
- Creating a Community Security Plan for Actions, Events, and Demonstrations

Disclaimer: The information provided in the Office Security and Safety Series are for informational and resource purposes only and not for the purpose of providing legal advice.

De-escalation Methods and Tactics

Social justice organizations have to think about the safety of their employees and members of their organizations at all levels. This includes adopting safety protocols to de-escalate tense situations at organization events, demonstrations, within your office, and from law enforcement.

This guide is designed to give you basic tips that will help train you and your staff to de-escalate tense situations. The act of de-escalating takes lots of practice and not all tactics work the same every time. The art of de-escalation also relies on your instinct.

Much of the information in this memo is from **Vision, Change, Win** and we are grateful for their contributions to this topic!

Most people at some point in their lives have de-escalated violence verbally. These tips build upon life skills, de-escalation experiences, and trainings that we have received from people in a wide range of professions. The skills to intervene in violence are the foundation for community safety work whether we're working to increase safety at organizational events, demonstrations, within our offices, violence in public (i.e. bystander intervention), and from law enforcement. Verbal de-escalation has some core principles but also varies widely depending on the situation, people involved, relationships between those people, and how everyone is being perceived. This document is a guide for your principles and practice, but not every tip will work every time or work the same. Instead use these tips to guide your practice by using these tips in a variety of situations and incidents to build your instincts.

Choosing to Intervene: Before you decide whether to intervene and how, it's important to thoroughly assess the situation.

Here are some questions to think about for a general assessment:

- **Assess** the risk to your personal safety.
- **Consider** your relationships to people involved and how people may perceive your involvement.
- **Consent:** How do you know it's OK to intervene?
- **Impact:** What are the costs or benefits of the situation? How will you make sure you don't make things worse?

In an office situation, you also need to assess the following:

- What is my organization's protocol for de-escalation?
- Do I need to call an emergency point of contact within my organization?
- Does this situation fall under how my organization defines crisis and does the organization's crisis management plan need to be followed in this case?

Tips on Verbal De-escalation

These tips were written with adapted contributions from Jewish Voice for Peace's "De-Escalation Manual."

Verbal De-escalation Tactics:

- **Prevent:** Most conflicts have indicators – tension, individuals with a history of conflict, voices raising, or a crowd growing around people. Use all of your senses and previous knowledge to anticipate conflicts or violence and reduce potential conflicts, separate people, reassure people, or create conditions for increased safety.
- **Active Listening:** When people are in conflict or being aggressive to others they often do not feel seen or heard. Use your body and facial expressions to fully take in and listen to the person or people. Reflect back to the person what you're hearing, "I hear that you feel..." Etc.
- **Empathize:** When a person feels validated it can reduce tension and increase their ability to follow directions, receive accountability, or negotiate a situation. Focus on speaking to the person from their perspective. Use phrases like, "I understand how that is hard," "I agree with you that....," "You're right, that is a problem."
- **Evade/Escape:** Sometimes the best way to de-escalate a situation is to evade or escape it, or to help a person who's being targeted to get away. Evading can be moving yourselves and other affected people away from the incident to a safer space. Or if you're witnessing harassment or violence one way you can help people escape by pretending to know them, "hey it's so good to see you." To start a conversation with the person to begin to see what sort of support they could use. Use additional tactics like distraction or gathering people to assist you in being able to move yourself or targeted individuals away from harm.
- **Distraction/Refocus:** Distraction can be a way to de-escalate a situation without having to be in close proximity. Loud noises from a distance, flickering lights on or off from a nearby building, can be ways of de-escalating from afar. Distraction up close can be about refocusing the person or conversation, ask them to take a walk with you. Or, propose an alternative plan or idea.
- **Gather People:** People act differently when there are other people observing. If you're de-escalating a situation in an area where there are more people you can bring people towards the situation. You can also mention the incident. "Do you see what's happening over there? This isn't ok. That person looks like they need help."
- **Use Humor:** Humor can lighten a situation and make people feel more connected and compassionate towards each other. Especially if you can make a person who is acting aggressively or causing harm to laugh. However, a note of caution, using humor to condescend or belittle someone can escalate a situation.
- **Give Choices:** When people are in the midst of causing harm or harassing people, they can be very sensitive to power dynamics, and can sometimes feel like they have limited choices. You can still give people choices that allow them to operate within conditions that create more safety for everyone. You can make statements like, "I need to ask you to either stop yelling, or move into the other room."

- **Use Your Voice:** Your vocal tone, the pace that you're speaking at, and volume can be used to convey a calming presence, respect, or power as needed. When a person is being aggressive or agitated, it can help to speak slightly slower or quieter than them while focusing on them. This will encourage them to work to listen which may make them more present and able to listen to your directions or the boundaries of others.
- **Body Language:** Similarly to using your voice posture, eye contact, and body language can convey a series of messages to another person. Having open arms and ensuring your hands are visible can de-escalate a situation. Slower movements can also work as well. In some instances, conveying authority by making yourself taller, speaking louder, putting your shoulders back, and pushing your chest up, can be helpful. For other situations a less powerful and more submissive stance including lowering shoulders, concave chest, eye contact that is focuses on the nose as opposed to the eyes, can increase a person's sense of safety. Use your instincts and your previous experiences to know which to use. Sometimes you will use several different stances within one instance.

Verbal De-escalation Tactics with Law Enforcement:

De-escalation tactics will differ when dealing with law enforcement. The best way to handle any type of situation that involve law enforcement is the following:

- Know in advance if law enforcement will be present at an event.
- Have an assigned point of contact who is trained and comfortable with talking with law enforcement.
- Know what your rights are and follow recommended protocol in 'Know your Rights' guides. A list of organizations who host such guides can be found in the 'Other Resources' section below.

Use Your Body Language:

Similarly, to using your voice posture, eye contact, and body language can convey a series of messages to another person. Having open arms and ensuring your hands are visible can de-escalate a situation. Slower movements can also work as well. In some instances, conveying authority by making yourself taller, speaking louder, putting your shoulders back, and pushing your chest up, can be helpful. For other situations, a less powerful and more submissive stance including lowering shoulders, concave chest, eye contact that is focuses on the nose as opposed to the eyes, can increase a person's sense of safety. Use your instincts and your previous experiences to know which to use. Sometimes you will use several different stances within one instance.

Escalators: Stay away from the following traits, as these tend to escalate the situation.

- | | |
|-------------------------------|---|
| • Aggressive body language | • Arguing |
| • Not listening | • Invading personal space |
| • Criticizing | • Assuming Identity/Categorizing People |
| • Name calling | • Trapping someone's exit |
| • Engaging in power struggles | • Shouting |
| • Ordering | • Interrupting |
| • Threatening | • Photographing/Filming People |
| • Minimizing | |

Verbal De-escalation at Protests or Events

In addition to the de-escalation tactics outlined above, there are a few other tactics that are unique to protests and events.

Before we go into those teams, always make the assumption that there will be police or counter-protestors present and either can be rude, violent, or agitated.

Assessing Safety

Some protests and events involve a large number of participants that may not be manageable. As a community organizer or activist, your first instinct is to try to de-escalate the situation. In some cases, you have to assess if you and your staff/colleagues need to run and remove yourself from the situation. When in doubt, walk away.

Added Security

If you are hosting an event that is sizable invest some time in ensuring security is in place to protect all of the participants. This usually involves making a security plan, training people to meet your protocols, and or hiring an external security team if you don't have internal capacity.

Always take time to plan and talk through all the options with your team. Understand which circumstances you would or would not call emergency services. Whether you use an internal or external security team, make sure the security team is trained to know your organization's values, emergency protocols, and aware of any crisis management plans you have in place.

Again, in these situations, your team should also always know what their rights are, and what any potential risks are. Please refer to the 'Other Resources' section for a list of organizations that provide this information.

Do Your Research

A key way to de-escalate situations is to prevent confrontation in the first place. To do this, know what the laws are for demonstrating, make sure you have the right permits for your events (this includes permission for food at the events), etc. If you follow the guidelines and are well-versed on what they are, this can help when confronted or asked about any logistics.

De-escalation of Office Incidents

Have a clear safety protocol for your office is important for ensuring the safety of your staff and volunteers. This is particularly important if you are an organization that addresses social justice issues or serves members of marginalized or heavily criminalized communities.

For more information, see subsection "Tips on Creating Office Safety Protocol."

Tips on Creating Office Safety Protocols

These tips were written by Vision Change Win Consulting with adapted contributions from the ACLU's "Know Your Right: Stops and Arrests – What to do When Encountering Law Enforcement."

For organizations whose members or clients are members of marginalized or heavily criminalized communities, it's essential to create and maintain safe office environments without law enforcement reliance or involvement. By marginalized and heavily criminalized communities, we're thinking of communities who experience discrimination and oppression from the government and law enforcement/immigration enforcement violence including: communities of color, lesbian, gay, bisexual, transgender, and gender non-conforming communities, people engaged in street economies such as sex work or drug sales, immigrants, people with disabilities, low-income communities, people living with HIV/AIDS, homeless communities, formerly incarcerated people, etc.

At any organization verbal conflict, physical fights, threats, or law enforcement violence or harassment can occur. This tip sheet is a starting point for organizations to think about how to create organizational safety protocols that do not rely upon law enforcement.

Organizational Safety Planning

- **Conduct an inventory.** There may be people in your organization with experience in verbal or physical de-escalation, self-defense, safety planning, know your rights trainings, copwatch, first aid, bystander response, and many other skills that are directly relevant to creating organizational safety. Conduct an inventory of your staff's skillset to learn about their experience and also their comfortability with navigating incidents of harassment and violence that could occur at your organization.
- **Create safety guidelines and values.** Create and publicly share your guidelines and values around safety in your space. For example, what's your position on banning people from your organization in the office? Or are staff expected to de-escalate and intervene in violence? What is your organization's position on calling law enforcement for violence? How do you want to address suicidal people within your office space? What information do you keep in your office that could be used to target or create risk? What data/information do you collect and who has access to it?
 - These guidelines can include:
 - Keeping the front door locked at all time and have a system in place where the front office staff can view visitors when they knock.
 - Making sure all visitors sign-in upon entry.
 - Have a clear policy of how to handle visitors who seem angry/upset. This can include having a point of contact who is trained in de-escalation tactics to manage and asking the person to wait outside until that person is present.
 - Training staff on all the guidelines.
- **Create safety protocols.** Based upon your inventory, guidelines, and values create some protocols on addressing violence in your space. Protocols should address topics including:
 - Types of harm and violence that the organization will intervene in
 - Supporters, organizations, allies that the organization can rely upon for additional help for various scenarios

- Point people in charge of making decisions during an incident based on scenarios
- Communication protocol for notifying people in the space about an incident (i.e. a code word, email that goes to all staff, or an announcement that occurs)
- Common scenarios that have occurred with sample responses.
- Identify gaps in skill set that might be needed based on scenario planning. For example, if a scenario requires dealing with a community member who is suicidal then a suicide intervention training may be helpful tool
- Determine exit strategy for scenarios that require getting folks in and out of the office.
- If your space uses intercoms or any video equipment to identify people as they come in and out of the space – consider any benefits/challenges to protocols this may offer.
- **Implementing safety protocols.** Once your protocol has been created regular trainings and scenarios practices should occur (at least 2x per year) so that staff can get experience in implementing the protocol. The protocol should be reviewed with new staff as a part of a new staff orientation process. And the protocol should be reviewed annually. Organizations can consider including the protocol in your policies and protocols manual.

Law Enforcement Visits: Whether it's random, connected to the communities that you organize, or connected to political backlash, all organizations should have a plan in place to address law enforcement visits. There are various types of law enforcement visits including visits to investigate your organization or a member of your organization, general inquiries, emergency response, and visits to "support." Protocols can differ based on the type of visit. Here are some general tips to guide you.

- **Physical Space.** An office space with a door that closes, and a staff member trained in de-escalating violence and navigating law enforcement near that door can make a huge difference. When possible consider spaces that make this possible.
- **Warrant.** You do not need to let law enforcement in without a warrant. Make sure that this warrant is signed by a judge, for the correct organization, and correct address. Ask to see the warrant before letting the officer inside. However, you do need to let officers inside if they come with paramedics or other emergency services.
- **Probable Cause.** Law enforcement can enter your space if they have reasonable suspicion of illegal activity happening inside. Keep this in mind as you craft your safety and de-escalation protocols.
- **Point Person.** There should be an organizational point person to navigate law enforcement. This person should be well aware of their legal rights and should be less vulnerable to arrest than other staff or community members, if possible. Vulnerability to arrest can include many factors including but not limited to: open cases, immigration concerns, having a criminal record, and identifying as a person of color, trans and gender non-conforming.
- **Careful about what you say.** Say as little as possible when dealing with law enforcement. Everything that you say can you be used in court. It's helpful to have talking points for various scenarios that you can stick to, this will minimize sharing information that could be used against you later.
- **Videotaping the encounter.** Consider having staff who are not the point person video the encounter. Know that sometimes cameras can escalate and de-escalate law enforcement but can also deter illegal and violent behavior on behalf of law enforcement and support a future legal case.
- **Seek support if needed.** If and when possible notify your legal support (if you have it), a close organizational ally, etc. in the case you need further support or want someone to check in with later.
- **Get the officer's Information.** Police officers legally are supposed to give you their names and badge numbers when asked. If they don't offer it freely try to capture what you can remember including what precinct they are coming from and what they look like.

- **Documentation.** After the police leave, be sure to write down anything that was said or occurred. If there were several folks in the space when they were there, ask them to also write down their account of what happened as well.

Other Resources

For more information about understanding what your rights are in dealing with law enforcement, Immigration & Customs Enforcement (ICE), we recommend familiarizing yourself with resources provided by the following organizations:

- American Civil Liberties Union publications: <https://www.aclu.org/know-your-rights>
- National Day Laborer Organizing Network: www.ndlon.org
- National Lawyers' Guild: www.nlg.org

Office Safety Sample Inventory

1. Do you have self defense or martial arts experience?

_____ No _____ Beginner _____ Intermediate _____ Expert _____ Trainer

Explain: _____

2. Do you have verbal de-escalation or bystander intervention experience?

_____ No _____ Beginner _____ Intermediate _____ Expert _____ Trainer

Explain: _____

3. Do you have experience with physical de-escalation?

_____ No _____ Beginner _____ Intermediate _____ Expert _____ Trainer

Explain: _____

4. Do you have experience with counselling or safety planning?

_____ No _____ Beginner _____ Intermediate _____ Expert _____ Trainer

Explain: _____

5. Do you have experience with police negotiation, copwatch, or know your rights trainings?

_____ No _____ Beginner _____ Intermediate _____ Expert _____ Trainer

Explain: _____

6. Do you have experience assessing people for suicide or homicide risk?

_____ No _____ Beginner _____ Intermediate _____ Expert _____ Trainer

Explain: _____

7. Do you have experience with first aid, CPR, or other emergency medical support?

_____ **No** _____ **Beginner** _____ **Intermediate** _____ **Expert** _____ **Trainer**

Explain: _____

Beginner = less than one year, learning basic concepts

Intermediate = 2 – 3 years, comfortable with basic concepts

Expert = 5+ comfortable with basic, intermediate, and advanced concepts

Trainer = I have intermediate to expert experience and substantial experience developing curriculum and giving training on this subject

Office Safety Planning Worksheet

For organizations whose members or clients are members of marginalized or heavily criminalized communities, it's essential to create and maintain safe office environments without law enforcement reliance or involvement. By marginalized and heavily criminalized communities, we're thinking of communities who experience discrimination and oppression from the government and law enforcement/immigration enforcement violence including: communities of color, lesbian, gay, bisexual, transgender, and gender non-conforming communities, people engaged in street economies, immigrants, people with disabilities, low-income communities, people living with HIV/AIDS, homeless communities, formerly incarcerated people, etc.

What are your organization values and how do they inform these safety protocols? <i>(What's your position on banning people from your organization in the office? Or are staff expected to de-escalate and intervene in violence? What is your organization's position on calling law enforcement for violence? How do you want to address suicidal people within your office space? What information do you keep in your office that could be used?)</i>	What skills do they staff currently have that can be used to navigate and address incidents around safety that may occur? What gaps exist and how will you address them? <i>(see attached inventory assessment worksheet)</i>
What are factors that might make creating and implementing safety protocols challenging? <i>(my office is isolated, there is no security in the building, we are renting a space, etc.</i>	What types of harm are you most concerned about that require developing a safety protocol? <i>(Please see office safety tips handout for guidance)</i>

At any organization verbal conflict, physical fights, threats, or law enforcement violence or harassment can occur. This worksheet is a starting point for organizations to create organizational safety protocols.

Please be advised that you may be inserting sensitive information in this worksheet that you might not want particular individuals to see. Therefore, it's important to think through what you want to have a verbal discussion about, and what information is safe to have written.

Creating Safety Protocols		
	Example	Your Scenario
What is the situation occurring?	There is an individual who keeps threatening to come to the office and harass our organization because they don't agree with the work we organization does. We know their name and we found a picture of them on their FB page. We have an open office space and no security in our building.	
What are warning signs that this situation is about to occur? (long term, short term)	The harassing emails and phone calls have increased from a few times a year to almost weekly. They've gotten more specific recently about what they are planning to do once they arrive at the office.	
Who is the point person/people who are responsible for engaging in the situation?	In this order: Josephina, Director Maria, Communication Coordinator Joseph, Social Media Coordinator	
How are the point people notified that they are needed?	When the person who has threatened harm arrives (we'll know because we have a pic), the first staff that sees them will say loudly "The water delivery from Poland spring is set to arrive tomorrow"	
How will they engage in the situation? What strategies will they use? What strategies will you avoid, not use.	The point person first available will engage the person by actively listening to them, and allowing them to vent so long as it doesn't cause harm. If a solution is possible, the point will negotiate. If not, the point will team up with another point person and attempt to get the harasser to leave.	
What are the desired outcomes of these intervention strategies?	To have the harasser leave the office feeling heard and seen and not needing to harass or complain anymore. That the staff in the office remain safe and that law enforcement is not	

	called in.	
While the point person(s) are intervening what are other staff doing? What should other staff not intervening NOT do?	Remaining staff are in the office, and not engaging with this person. They are being cautious and observant and ready to call in further support if needed. If a client is in the office they are helping them to exit safely.	
In the case, these interventions are not successful what will happen? (Call for support? Trigger an alarm? Call the police?) Be sure to define how you know an intervention is not successful.	In the case an intervention is not successful, we will call for x organization to come to the office to support with further intervention strategies. The goal will be to get the harasser out of the office. We know they are needed when the point person, says "Please call x and let them know I'm going to be late for my meeting."	
Is an exit plan required? If so what is the plan? Who will support the implementation of the exit strategy? After folks exit how will they check in? Where will folks convene to check in?	If the harasser refuses to leave and/or is escalating in violence, then 2-point people should remain and the 3 rd point person should gather remaining folks in the office to exit quietly and wait in the parking lot. The 3 rd person should and post themselves outside the office door to wait for further support.	
Support: Who should be notified of what's happening? What are/is their role and contact info?	These 3 people should be notified if this scenario occurs: Board chair, 2 outside support people. We are letting the board chair know what's happening, and asking the support people to be on standby in the case we need them to physically show up.	
If you decide to call upon law enforcement: What determining factors will initiate involving them? Who will be point to engage with them? What is the plan to reduce potential harm when engaging with law enforcement?	We will only call law enforcement in the case physical violence occurs or the if we are being threatened with a weapon. Joseph will intervene with the police should we call them. To reduce harm, we will ask our support team to be physically present and release the rest of the staff to go home and wait for further instructions.	
Documents/other materials/information to consider having alongside this plan: name of legal support, management contact info, building floor plans, staff emergency contact info etc.	Support team contact info, point people cell phone numbers, board chair cell phone numbers, information on the harasser that we gathered from social media.	

Entrapment Protection

Entrapment and entrapment attempts of social justice organizations/leaders is on the rise and can have serious consequences.

**Always exercise awareness and caution to what is said aloud or sent via email.
Do not say anything that you would not want to be public or end up in the news!**

Every nonprofit organization should have a list of protocols that clearly outline how to manage everyday walk-ins and phone calls to their office(s) that fit in line with the organization's values. This includes policies and procedures on how to track messages and field calls from important stakeholders. This particular document acts as a supplement to those protocols and solely focuses on how to manage individuals whose intent is entrapment.

In this document, entrapment refers to someone pretending to represent an entity falsely, the act of an individual trying to induce a member of your organization to make a statement or commit an act that can be used against the organization. For example, this could be the case when an individual takes a statement out of context and uses it in a smear campaign against your organization. Another example includes paid informants trying to encourage a member of your organization to commit a crime. Please note, RoadMap sometimes also refers to entrappers as "posers." For the purposes of consistency in this document, we will be using the word entrappers.

The same groups that seek to entrap members of your organization may also be working to entrap members of the community your organization serves. There are separate protocols your organization can take to identify these cases and help educate your community on how to handle those situations. Although this is an important topic to discuss, handling this type of situation is not covered in this document. For additional information, please refer to RoadMap's document entitled, "Event Security Plans."

Role of the Receptionist/Office Administer

The front staff of your organization, usually the receptionist or office administrator, will often be the first one to encounter a walk-in or a call-in. This staff member should be empowered with the necessary training and support to execute the protocols you create. At the same time, dealing with office security and safety are big tasks to tackle and it should not be the expectation that the receptionist or office administer manage it by themselves. There should be an expectation that other staff will be involved to assist with the de-escalation of different scenarios that may come up and decision-making when needed.

Keys to Success: Important ways to Proactively Prepare

To be fully prepared to respond to cases of entrapment or posers, we suggest that your organization have clear messaging that can be used in various types of cases. This messaging would clearly outline your organization's mission, values, and the work it does. This messaging should be designed in a way so it can be used in any type of situation (media requests, fundraising, managing crises, and so on). This messaging is often created as part of a crisis communication plan.

Additionally, it would be helpful to have a clear emergency plan to implement when there is a case of entrapment. This plan would include identifying which key members of staff would be notified and

tasked with creating and implementing a strategy to manage the case. This is often called a crisis management team and they would implement the protocols outlined in a crisis management plan.

For support in this area, RoadMap has additional resources that can guide your organization to create both a crisis communication and crisis management plans.

What to Look For?

When dealing with callers or walk-ins you want to look for specific signs that indicate that extra precautions should be taken when communicating with this individual. However, not all callers or walk-ins will carry these characteristics and you should assume that any conversation you have with someone could lead to a possible entrapment case. Therefore, stay on message and be mindful of what you say at all times. With that being said, the signs listed below may help flag possible scenarios. The protocols in this document should always be implemented and followed to protect your organization.

Signs to look for:

- Refuse to give their name or contact information.
- Not clear on the purpose of their call or visit.
- Make statements that appear to be intended to incite a reaction (i.e. they support some type of violence or marginalization of a community).
- Ask leading questions or make inflammatory or provocative statements.
- If you are a client-based organization, their case may seem not plausible.

Structure of Reception Area

- Decide who from the organization will greet walk-ins and answer the phone calls. If you do not have a designated reception or office administrator, it is recommended that not everyone answer the phone or be tasked with greeting walk-ins. Rather, have a few selected staff members who are trained in these protocols. Whoever is tasked with managing walk-ins and answering the phone calls, should also be capable of handling stressful situations and there should be a protocol, a system, special code or alert mechanism to alert other staff or higher ups to step in and handle the situation when needed (i.e. a crisis management team). Alternatively, you can train these staff on de-escalation tactics.
- Consider adopting a policy for how walk-in requests will be responded to. We strongly suggest requiring all walk-ins to sign in. Other policies may include:
 - Ensure the sign-in sheet is reviewed immediately when filled out.
 - The organization only meets with community members by appointment.
 - For organizations that are client-oriented, ask them to fill out an intake form that can be reviewed before a staff member meets with them.
 - Ask for guests to show identification.
 - *Note: These are only examples and may need to be catered to fit your organization.*
- If they are requesting to meet with a staff member and you do not know the person, take the following steps:
 - Do not immediately inform them that the person is present or available.
 - See if you can do a quick search on the person and if any red flags (research elaborated on below).
 - The safest step to take is to tell the person the employee they requested to see is not available and you will call them back to set up an appointment. This gives you more time

to research the person properly. To help, consider placing some type of barrier between the reception desk and the rest of the office so an individual who walks in cannot easily get through. The trick is to make sure that the employee who the individual wants to see doesn't come to the reception area during this time.

- If the team feels like the meeting should take place immediately, meet in a conference room or a room that does not have any papers, filing cabinets, etc. with sensitive information and have at least two people in the meeting. You can also consider recording if the team feels it is necessary (recording is elaborated on later).
- For some communities, entrapment tactics are used by law enforcement, particularly when they are searching for specific information. As you should know, anything you say or do in front of law enforcement can be used against you or your organization, and therefore, any visits need to be handled properly. In instances where law enforcement appears without being called or Immigrant & Customs Enforcement (ICE) officials appear there should be clear protocols for who and how this is handled. These types of unexpected visits can be frightening. We strongly recommend that your policy does not place the responsibility for managing police relations or receiving or evaluating warrants to reception staff. Consider having protocol that front office staff are tasked with saying they are not authorized to evaluate a warrant or grant access and that they will call on someone who is to speak to them. These interactions are covered in more detail in other RoadMap materials and webinars.

How to Communicate with the Caller or Guest:

- For phone calls, always ask the full name of the caller, their contact information, and the purpose of the call. Consider having an intake form that creates an official way to document 'suspicious' conversations. Report these "suspicious" calls to your Crisis Management Team.
- For walk-ins, always have sign-in sheets that require listing their name, contact information, and purpose of their visit.
- Be extremely cautious about what you say or write to the person and never give information out that cannot already be found on your website or a recent publication (i.e. press release).
- If they insist on additional information, refer them to your website.
- Never send any information over email that is outside of your official messaging (as we explained in 'Keys to Success' section).
- Always document and record any interactions with suspicious guests and keep for record keeping.

Researching

We have suggested a few times to do some research on the person in question. This research can primarily be done through a basic web search. Here are some things to look for:

- Quotation in other articles that share more information about who they are and what their views are.
- Verify their credentials are accurate.
- If you are a client-based organization, create a process to verify claims as part of the in-take process.
- Look for public posts on social media that may be concerning (i.e. strong statements that are against the community your organization serves or the cause your organization supports).

- Find ways to verify their name is real. One way would be to find social media and take the following steps:
 1. Find a picture of them on social media platforms and download it if you find one.
 2. Open a search engine on a browser and find the option to search for images. Follow the steps it provides.
 3. See if pictures of the same person come up with a different name.

What to do post research?

If the research indicates that this person may not be who they claim to be, find ways to decline their requests. For example, you may tell the person that someone will get back to them and never follow up. In most cases, the entrapper will not follow through.

If for any reason you believe this person may also approach organizations that are your partners or allies, consider telling them about this incident so they can be prepared as well.

Interview Requests

If they are asking for an interview, always take a message and communicate that someone from the organization will get back to them. This will give you a chance to research the person and find any flags that may indicate what their intent is. Make sure to always ask for credentials and what their deadline is. In the event that they do represent a media entity, you always want to help them meet their deadline. It is possible to help them reach deadlines and still follow the protocols outlined in this document.

If they say they are an independent reporter or a freelancer, ask them for samples of their work in addition to researching them.

If you do not find anything that confirms the person's claim or your suspicions after research, always trust your gut and be very cautious about what you say or write to that person. If you still do not feel comfortable giving an interview, ask the person to email the questions and answer over email. This is where clear messaging comes in hand as you can repeat the organization's messaging over and over again. There is no harm in sticking to this messaging and you won't lose an opportunity if it is a legitimate media request.

If you proceed with this option, keep a copy of the email for your record keeping.

If you decide to move forward with an in-person interview, you can still use the strategy of repeating the organization's message over and over again.

Lastly, one or two staff members who are trained to deal with different types of interview scenarios should handle all interviews.

Issues around Recording

When protecting your organization from potential cases of entrapment, your organization should adopt policies that indicate when it is okay to record and how to handle situations when you are being recorded.

When to record?

When in doubt, always record a conversation so you have a copy of the conversation for your own records. This can help clarify any statements that may be taken out of context and provide proof against any accusations that may be made against your organization.

However, you must be familiar with your state's laws on what consent is needed when recording. Currently (as of 1/1/2018), 12 states forbid the recording of private conversations without the consent of all parties. This includes California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington. Make sure to continuously check the laws for any changes.

If you live in a state that needs the consent of all parties, try documenting the conversation that is happening by taking detailed notes via pen and paper or typing. If that is not possible, document the conversation after the conversation has concluded. It may even be a good idea to create a template form that staff fill out (aka an in-take form) so all details are documented correctly and thoroughly.

When they are recording you

If they are recording openly with you, you have the right to decline to be recorded or ask them to not record.

If you feel you are being recorded secretly in your office, you can also ask them if they are recording or indicate they do not have permission to record. Even if they deny they are not recording, repeat that they do not have permission to record and make no other comments.

If you feel you are being recorded in a public space, you can decline to make any comments or make comments that are short and concise and match the organization's messaging or already found on your website. For example, a short response that may already be part of your messaging is 'The tax bill favors the wealthy over the rest of us.'

This may be an opportune time to record any comments so you have proof of what you said. Or consider asking another staff member to join you and witness you making comments.

For these situations, it would be helpful to have clear policies that outline when people can or cannot record within the office. For example, you can have a policy that you only allow individuals with verified credentials to record. Alternatively, you can have a protocol that states no one is allowed to record. It could also be a good idea to post these policies somewhere where it is visible in the reception area of the office.

If you are a target of entrapment, know your legal rights and push back, when possible. There should be consequences for entrapment and entrappers.

Advocacy Statements

Make sure all staff are trained on the statements the organization can or cannot make regarding policies, elected officials, or candidates. Make sure all staff know they can never express their personal views when representing their organization. This includes posting personal views on social media. (For

more information check out the sample “Social Media Policy” in this Toolkit). Make sure all staff are clear on what messaging exists on advocacy issues the organization is currently engaged with.

Seeking Legal Assistance

If you feel your organization may be threatened with an entrapment case, you should contact an attorney for legal support and advice. It is important to establish relationships with attorneys ahead of time so you know who you can approach. Your organization can also look at social justice organizations who may provide legal services pro-bono such as the National Lawyers’ Guild or the Lawyers’ Committee on Civil Rights.

Creating a Community Security Plan for Actions, Events, and Demonstrations

These tips were written with adapted contributions from the Audre Lorde Project's "Security Training for Participants" and "Build a Protocol Workshop."

While the right to protest is legally protected, it's important to ensure actions, demonstrations, and events are the safest possible for the communities you organize within. This document outlines some key considerations and structures for security plans that organizations can create to increase safety at actions and events that do not rely upon law enforcement.

What is a Security Team?

- A group of people who are not directly participating in the action, demonstration, or event who are entrusted to keep people safe, ensure the action or event gets carried out successfully, and work to prevent or reduce arrests and harassment.
- A group that serves as a buffer between attendees and counter protestors and/or police

Creating a Plan:

Important Assumptions:

- If you're planning a demonstration or action (permitted or unpermitted) assume that there will be a police presence (whether seen or unseen), and that the police may be agitated, rude, violent, and could arrest people without cause.
- Assume that counter-demonstrators are a possibility. If you're in an open carry state assume that armed counter demonstrators are also a possibility.
- Assume that your community members may also get agitated, angry, or aggressive towards police, each other, or counter protestors.

Do Your Research:

- Know the relevant laws connected to protests in your state and city. What materials are legal and or illegal (i.e. types of signs etc.)? How much space is needed if you march on the sidewalk? Are permits required? Are there size specifications or permits needed for amplified sound?
- If your action is a march, walk the route for your march at a similar time of day and day of the week for your planned protest. Observe and notice how populated the area is, police presence, and any other relevant details. Determine if there are other possible events occurring in the area on the planned day of your march that may have an impact.
- If you're planning to do an action inside a private location that is not your office or a building that you have permission to do an action, review whether or not there are security guards, how many, and where do they tend to be located. Take note of entrances and exits, and whether special ID's are needed to enter the building. Remember that security cannot arrest you, but can call the police to arrest you.
- For private event spaces – including your office, research whether or not the space has a contract with a private security company and what the security protocols are of this company. Especially for event spaces it helps to pre-negotiate with private security that your team will be the first folks to navigate and de-escalate safety issues. It is also important to negotiate that any decisions to call the police should be done with the consent of your team. If you are working with communities that are heavily surveilled, policed, criminalized, (i.e. communities of color, LGBTQ communities, undocumented communities, immigrant communities, Muslim and Arab communities, homeless communities, low-income communities) you should consider doing an

anti-oppression training with the private security team to minimize unnecessary and/or oppressive conflicts that could lead to arrest.

Roles: There are several roles for a security team. Depending on the size of your team some roles can be consolidated.

- *Marshals* follow the direction of the tactical team and are often the first line of defense between the action/event participants and any threats or opposition
- *Police negotiator* a person designated to interface with the police, usually a member of the tactical team, makes decisions to carry out the event/action.
- *Legal Observers* individuals to observe, document, and ensure that the legal rights of protestors are being upheld.
- *Security Coordinator* a person who recruits the security team, trains the security team, creates the protocols with the program leads, decides the security formation, and often serves on the tactical team.
- *Captains* individuals who coordinate a small group of marshals. For large events captains can move a bit more freely than marshals (who are usually stationed in one area). Having captains can support decision-making.
- *Runner/Mobile Captains* people who are free to float through the march, action, demonstration etc. These people can act as the eyes and ears for the tactical team, can help communicate shifts and changes to captains and marshals as necessary, and can fill in gaps when they see them in the formation.
- *Tactical Team:* A small group of people including a program point person, security coordinator, and police negotiator that make day of decisions about the event, action, or demonstration including: whether individuals need to be removed from the event/action/demonstration, whether or not to change the route, how to navigate counter protestors, and how to navigate police or arrests. These individuals hold the organization's mission and values central in addition to the goals of the event when making these decisions.
- Tactical team members must be able to: communicate clearly, make quick decisions, be comfortable with making unpopular decisions, remain calm during tense situations, have security experience, have one role during the event (i.e. press greeter + tactical = bad idea), and understand the community well and have trust from the community.

The Plan: Here are some key components of a security plan.

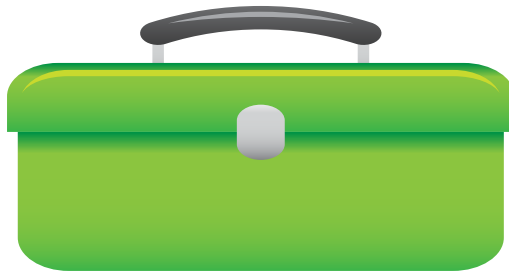
- History, Background information, and goals of the event/action/demonstration.
- Formation: Information on how security will be set up at the event/action demonstration. (i.e. will marshals be around the perimeter). Formations should be designed to create the most safety for participants and the most visibility for security.
- Scenarios: Any scenarios that security should expect based on your research
- Protocols: information on how security should navigate the scenarios.

Training the Team: There should be at least one training for the security team to review the plan and practice the relevant scenarios and protocols.

Key training components are:

- Training on what security is and what the roles are
- Training on Verbal de-escalation tactics and security guidelines
- Time to practice the formation, scenarios, and protocols

Section 6: Various Memos, Tools and Documents



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

- 6.1 *Understanding and Beating Back Opposition Attacks*
- 6.2 *C3 C4 Affiliated Organizations Transactions Flow Chart*
- 6.3 *Sample Acknowledgment of Ban on Nonpartisan Activities*
- 6.4 *How Worker Centers Can Keep 501c3 Tax Exempt Status*
- 6.5 *Fundraising—Charitable Solicitation in Multiple States Registration and Compliance*

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 3 rd 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.

<p>3. Accusations, complaints and/or investigations of voter registration violations/fraud</p>	<p>-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</p>
<p>4. Law suit(s) intended to censor, intimidate, financially burden or silence your organization or allies (strategic lawsuit against public participation=SLAPP suits)</p>	<p>--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.'"</p>
<p>5. Attempted entrapment/secret videotaping or audio recording</p>	<p>-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 Rights. Highly edited secret taping made it appear that CHIRLA director was laughing during the pledge of allegiance.</p>
<p>6. Threats of physical intimidation, violence, hate calls/mail/stalking</p>	<p>- Coalition for Humane Immigrant Rights (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,</p>

	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

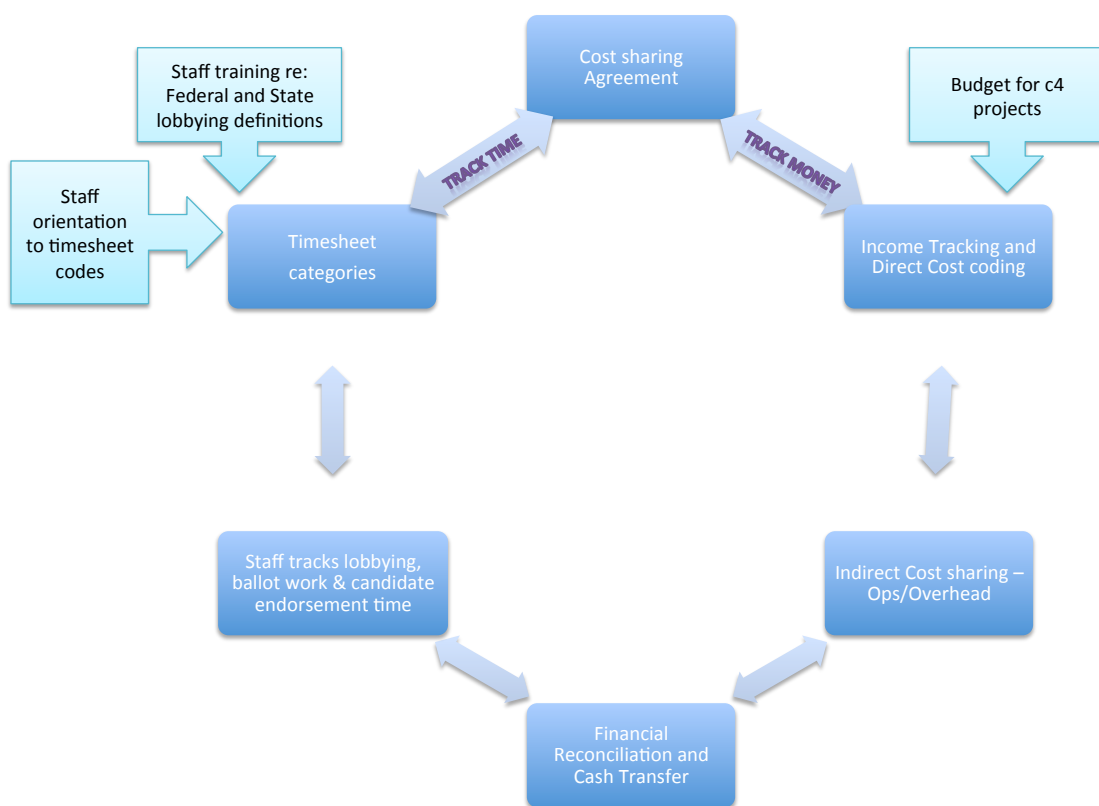
One thing you will note which all these forms and examples of attacks have in common. *None of the attacks are about the substance of the issues the social change groups are working on.* The issues they are effectively working on are the reason for the attacks, but the attacks are all about finding or 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

C3 C4 Affiliated Organizations Transactions Flow Chart



© RoadMap 2014

Sample “Cost Sharing Agreement”

Agreement for Allocation of Costs and Reimbursement of Expenses Between 501(c)(3) and 501(c)(4) Organizations

A 501(c)(3) and a 501(c)(4) may share employees, office space, equipment, supplies as long as 501(c)(4) pays its full and fair share of these costs. It is essential that there be a written agreement as to when and how much the 501(c)(4) will pay for its’ full and fair share of these costs. This is called a cost sharing agreement.

These costs should be paid regularly and within a reasonable time. While there is no clear IRS guidance on what is reasonable, a 501(c)(4) should reimburse a 501(c)(3), we recommend that expenses be reimbursed within 30 to 60 days. You should also consider charging a small late fee of 1% or 2% for expenses not reimbursed in a timely manner based on the agreement. The 501(c)(3) **must never subsidize**, in any way, the expenses of the (c) 4. This would jeopardize the tax-exempt status of the (c) 3 thus the importance of timely reimbursement. Below is a sample template for a cost sharing agreement.

SAMPLE: AGREEMENT FOR ALLOCATION OF COSTS AND REIMBURSEMENT OF EXPENSES BETWEEN

[Name of 501(c)3 organization] AND [Name of 501(c)4 organization]

THIS AGREEMENT is made this ____ day of (month____ (year), by and between **[501(c)3 Name] and [501(c)4 Name]**.

WHEREAS, [501(c)3 Name] is organized and operated for charitable and educational purposes within the meaning of section 501(c)(3) of the Internal Revenue Code (“Code”), including, but not limited to, (fill in mission); and

WHEREAS, [501(C)4 NAME] is organized and operated for social welfare purposes within the meaning of Code section 501(c)(4), including, but not limited to, conducting advocacy dedicated to (fill in) (example: social and economic justice issues; and (or such as____).

WHEREAS, [501(C)4 NAME] and [501(C)3 NAME] have agreed that it is in their mutual best interests to minimize duplicative expenses and to carry out their complementary purposes in an economical and efficient manner, including the sharing of employees whose skills and knowledge will assist both organizations and the sharing of office space and equipment;

NOW, THEREFORE, in consideration of these mutual promises and mutual benefits, [501(C)4 NAME] and [501(C)3 NAME] agree to share a variety of personnel, facilities, goods and services in accordance with the terms set forth below.

Section 1: Sharing of Personnel and Facilities.

1.1 Personnel. [501(C)3 NAME] shall make available to [501(C)4 NAME] the services of its employees, to the extent they are not otherwise occupied in providing services for [501(C)3 NAME], to perform a variety of administrative, program, financial, fundraising, and other similar functions for [501(C)4 NAME] on an as-needed basis.

- 1.2 Equipment and Facilities. To the extent that the activities of [501(C)4 NAME] are and remain consistent with the overall purposes and goals of [501(C)3 NAME], employees of [501(C)3 NAME] who are made available to [501(C)4 NAME] and employees and contractors hired directly by [501(C)4 NAME], if any, may use office space, office supplies, office equipment and furniture, and similar items of [501(C)3 NAME].

Section 2: Method of Payment.

- 2.1 Payment of Direct Costs. [501(C)4 NAME] shall pay [501(C)3 NAME] for all expenses incurred by [501(C)3 NAME] on [501(C)4 NAME]'s behalf. Such expenses shall include, but are not limited to, salaries and fringe benefits of [501(C)3 NAME] personnel who perform services for or otherwise assist [501(C)4 NAME] in carrying out its purposes, fees to independent contractors, the costs of travel conducted by employees and contractors, postage, computers, long-distance telephone charges, mileage, printing, and other actual expenses; provided, however, that [501(C)4 NAME] shall contract directly with vendors for the provision of such goods and services to the extent feasible.
- 2.2 Calculation of Payment for Salaries and Fringe Benefits. [501(C)4 NAME]'s payment for services of [501(C)3 NAME] personnel shall be based on the proportion of the salaries and fringe benefits of [501(C)3 NAME]'s personnel expended on [501(C)4 NAME]'s functions, as determined in accordance with time-sheets or other reasonable documentation prepared by [501(C)3 NAME]'s employees pursuant to instructions of management and agreed to by [501(C)3 NAME] and [501(C)4 NAME].
- 2.3 Payment of Overhead Costs. [501(C)4 NAME] shall pay [501(C)3 NAME] an additional amount to cover overhead costs, which shall be calculated by multiplying [501(C)3 NAME]'s total overhead costs by the percentage obtained by dividing the total staff hours charged to [501(C)4 NAME]'s activities by the total staff hours worked by all [501(C)3 NAME] staff. The overhead items to be reimbursed at this calculated percentage shall include, but are not limited to:
- a. costs of staff devoted to administrative matters, including, but not limited to, clerical, reception, and accounting activities, to the extent such costs are not accounted for under section 2.1;
 - b. storage;
 - c. equipment rental and maintenance;
 - d. depreciation of equipment and furniture owned by [501(C)3 NAME];
 - e. premiums for liability and other insurance;
 - f. general office supplies;
 - g. general telephone service, exclusive of long distance charges;
 - h. computer and word-processing supplies;
 - i. professional staff, board, and committee travel not accounted for under section 2.1;
 - j. photocopying not accounted for under section 2.1;
 - k. local taxes;
 - l. subscriptions and other publications;
 - m. rent and utilities;
 - n. Internet access costs.

If and when [501(C)4 NAME] shall use the services of any employee or contractor who is not also an employee or contractor of [501(C)3 NAME], [501(C)4 NAME] shall pay an additional amount of rent in proportion to these employees' or contractors' use of [501(C)3 NAME]'s office facilities.

2.4 Payment of Joint Fundraising Costs. [501(C)4 NAME]'s payment for joint fundraising costs incurred by [501(C)3 NAME] shall be based on the proportion of the amount raised for [501(C)4 NAME] in the fundraising effort.

2.5 Time of Payment. [501(C)4 NAME] shall make payment to [501(C)3 NAME] of the amounts due under this Agreement no less frequently than quarterly on the basis of detailed invoices submitted by [501(C)3 NAME]. Amounts in arrears for more than thirty (30) days shall earn interest at the rate of (2% suggested) per month.

2.6 Additional Payment in Event of Adverse IRS Determinations. In the event that the Internal Revenue Service ("IRS") determines that the amounts paid by [501(C)4 NAME] to [501(C)3 NAME] for goods and services pursuant to this Agreement constitute less than fair market value, then [501(C)4 NAME] shall pay to [501(C)3 NAME] the difference between the amounts paid under the Agreement and the fair market value of such goods and services as determined by the IRS. In addition, in the event that the IRS determines that all or any part of the amounts paid by [501(C)4 NAME] to [501(C)3 NAME] for goods and services pursuant to this Agreement shall constitute unrelated business taxable income within the meaning of Code sections 511-513, [501(C)4 NAME] shall pay to [501(C)3 NAME] the amount of taxes, penalties and interest, if any, determined by the IRS to be owed by [501(C)3 NAME] with respect to such income.

2.7 Change in IRS Requirements. It is the intention of [501(C)4 NAME] and [501(C)3 NAME] that the method of calculating [501(C)4 NAME]'s share of the expenses incurred by [501(C)3 NAME] on its behalf shall conform in all material respects with the requirements imposed by the IRS with respect to similarly situated organizations. In the event that [501(C)3 NAME] is advised by counsel or other tax advisor that the method of calculating [501(C)4 NAME]'s share of expenses set forth in this Agreement no longer conforms with such requirements, the Agreement shall be amended to conform with all IRS requirements.

Section 3: [501(C)3 NAME] Responsibility for Employees

3.1 Sole Responsibility for Employees. [501(C)3 NAME] shall continue to bear sole responsibility for compensating the employees, in accordance with its wage and benefit plans, personnel policy and all applicable labor laws. [501(C)3 NAME] shall continue to bear sole responsibility for payment of all applicable taxes, payroll deductions and other similar items, including but not limited to federal and state withholding taxes, workers compensation and unemployment insurance.

3.2 Relationship of Employees. [501(C)3 NAME] employees will, at all times, be and remain the employees of [501(C)3 NAME], and the employees will be considered neither independent contractors nor employees of [501(C)4 NAME]. [501(C)3 NAME] shall continue to be solely responsible for the terms and conditions of employees, whether the employees provide services for [501(C)3 NAME] or, at [501(C)3 NAME]'s direction under this Agreement, for [501(C)4 NAME].

3.3 Policies. In performing the services pursuant to this Agreement, employees are expected to follow and adhere to the written rules, regulations, directions and policies of [501(C)3 NAME].

3.4 Overtime. [501(C)3 NAME] shall be responsible for aggregating the total hours worked during each period for each of the employees, regardless of whether all or a portion of the pay period is spent

working on [501(C)4 NAME] activities and will be wholly responsible for meeting any overtime obligations under the Fair Labor Standards Act.

- 3.5 Reporting Performance Problems. [501(C)4 NAME] will report any performance problems or rule violations to the [Chief Operating Officer], and [501(C)3 NAME] shall handle all disciplinary matters of its employees.

Section 4: License of Marks.

- 4.1 Definition. For purposes of this Agreement, “[501(C)4 NAME]’s Trademarks” shall mean the registered and unregistered trademarks identified on Exhibit A hereto.
- 4.2 Grant. Subject to the terms and conditions herein, [501(C)4 NAME] hereby grants to [501(C)3 NAME] a non-exclusive, non-transferable, license for the duration of this Agreement to duplicate and use [501(C)4 NAME]’s Trademarks in connection with its activities in furtherance of its mission, subject to restrictions set forth in this Agreement.
- 4.3 Ownership. [501(C)3 NAME] acknowledges that [501(C)4 NAME]’s Trademarks are owned exclusively by [501(C)4 NAME]. [501(C)3 NAME] shall not use or authorize any third party to use [501(C)4 NAME]’s Trademarks except as approved in advance by [501(C)4 NAME].
- 4.4 Quality Standards. [501(C)3 NAME] agrees to maintain such quality standards as shall be prescribed by [501(C)4 NAME] in the conduct of the business operations with which the trademarks are used. [501(C)3 NAME] agrees to supply [501(C)4 NAME] with specimens of all uses of [501(C)4 NAME]’s Trademarks upon request. [501(C)3 NAME] shall comply with all applicable laws and regulations and obtain all appropriate government approvals pertaining to the sale, distribution and advertising of the goods and services covered by this License.
- 4.5 Infringement. In the event that [501(C)3 NAME] learns of any infringement or threatened infringement, or passing-off of [501(C)4 NAME]’s Trademarks or that any third party claims or alleges that [501(C)4 NAME]’s Trademarks are liable to cause deception or confusion to the public, [501(C)3 NAME] shall notify [501(C)4 NAME] and, upon [501(C)4 NAME]’s request, provide necessary information and assistance to [501(C)4 NAME]’s efforts to determine whether to commence or defend related proceedings, and to engage in such proceedings..

Section 5: Mailing Lists

[501(C)3 NAME] shall make its full mailing list available to [501(C)4 NAME] for [501(C)4 NAME] use and shall periodically provide [501(C)4 NAME] with updates to that list. In consideration, [501(C)4 NAME] shall provide [501(C)3 NAME] with all unique names on [501(C)4 NAME]’s mailing list. The parties will review the number of names each party has provided to the other party on no less than a quarterly basis. If at any time [501(C)3 NAME] has provided [501(C)4 NAME] with more names than [501(C)4 NAME] has provided to [501(C)3 NAME], and [501(C)4 NAME] does not make up that shortfall within thirty (30) days, [501(C)4 NAME] shall compensate [501(C)3 NAME] for the **fair market value** of the list exchange shortfall. Each party shall routinely notify the other party of any change of name, address, email address or any information that it learns about an individual on either list.

Section 6: Miscellaneous.

- 6.1 Termination. This Agreement may be terminated by either party at any time, upon provision of thirty (30) days' notice in writing to the other party.
- 6.2 Integration; Modification. This Agreement sets forth the entire agreement between the parties, and replaces and supersedes all other contracts, agreements and understandings, written or oral, relating to the subject matter hereof. The Agreement may not be changed or modified except by written instrument executed by both parties.
- 6.3 Governing Law. The Agreement shall be construed and interpreted in accordance with the laws of the State of _____ without regard to its conflict of law provisions.
- 6.4 Effective Date. The provisions of this Agreement shall apply to all applicable expenses incurred since [month, date year]

IN WITNESS WHEREOF, the parties hereto have signed their names on the day and year before mentioned.

[501(c)4 Name]

[501(c)3 Name]

By: _____, President

By: _____, Chair

Note: Keep good documentation of all share costs and how value of these costs and services was determined. For example, document how you determined the "fair market value" of lists/names purchased. Currently, the FMV is \$40.00 - \$60.00 for 1,000 names. (January, 2018)

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

Combat discrimination

Improve public health and social welfare

Provide research and public education on subjects beneficial to the community

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

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 you 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 as 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:

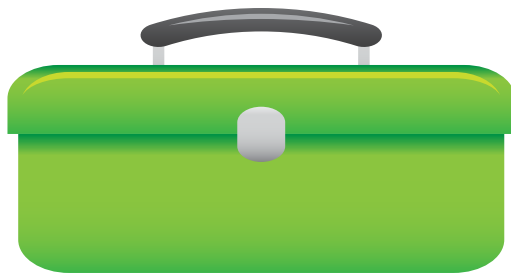
- Find the states that regulate charitable registration [from this map](#).
- Find your [state agency responsible for regulating fundraising activities](#). The charity official varies from state to state.
- Forms and requirements for registration and reporting vary from state to state. Use this link 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.

This product was created by members of RoadMap
Creative Commons Attribution License



Attribution-ShareAlike
CC BY-SA

Section 7: 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.

- 7.1 Must Read Resources
- 7.2 Helpful Websites and Contacts
- 7.3 My Healthy Organization
- 7.4 Getting IT Support for Your 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 find additional information at <https://roadmapconsulting.org/consulting-services/wts-public/>. Please contact weather@roadmapconsulting.org with any questions.

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

Section 7: Must Read Resources, Websites and Email Addresses

- ["Digital Security for All"](#) by Equality Labs

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 <https://roadmapconsulting.org/resources/>.



Helpful Websites and Contacts

[Fun with Financials](http://www.funwithfinancials.net) – <http://www.funwithfinancials.net>

[MAP for Nonprofits](http://www.mapfor nonprofits.org) – <http://www.mapfor nonprofits.org>

[Political Research Associates](http://www.politicalresearch.org) – <http://www.politicalresearch.org>

[Financial Accounting Standards Board](http://www.fasb.org) – <http://www.fasb.org>

[Alliance for Justice](http://www.bolderadvocacy.org) – <http://www.bolderadvocacy.org>

[Camino PR](http://www.caminopr.com) – <http://www.caminopr.com>

Andrea Hagelgans – ahagelgans@caminopr.com

[RoadMap](http://www.roadmapconsulting.org) – <http://www.roadmapconsulting.org>

Emily Goldfarb, Director – emily@roadmapconsulting.org

Michelle Foy, Program Manager – michelle@roadmapconsulting.org

Request Services – <https://roadmapconsulting.org/request-services/>

[Harmon, Curran, Spielberg + Eisenberg, LLC](http://www.harmoncurran.com/) – <http://www.harmoncurran.com/>

Beth Kingsley – bkingsley@harmoncurran.com

[My Healthy Organization Online Assessment Tool](http://myhealthyorganization.roadmapconsulting.org/) –
<http://myhealthyorganization.roadmapconsulting.org/>



My Healthy Organization and Our Healthy Alliance Online Assessment Tools 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 these online tools, [My Healthy Organization \(MHO\)](#) and [Our Healthy Alliance](#) are ideal assessment tools for organizations and alliances 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 webinars 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 <http://myhealthyorganization.roadmapconsulting.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...

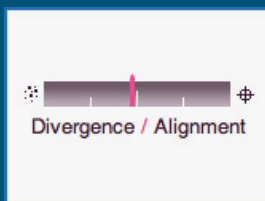
My Healthy Organization is an ideal assessment tool for organizations that are:

- ❖ 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:



- ✓ Is there a clear and compelling organization's existence?
- ✓ Are there differing or opposing...
- ✓ Are the mission and vision he... understood organization-wide
- ✓ Have you articulated the core...

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.

Getting IT Support for Your Organization

From Information Ecology (updated 8/2017)



This work is licensed under the [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

Types of support

Managed services

What it looks like: Proactive regular maintenance (software updates, antivirus, etc.) and troubleshooting in response to requests relating to all networks, equipment, and operating systems within an organization. Can also include other software by agreement, but generally does not include all applications installed on devices. Managed services companies generally have systems by which they provide updates and support remotely, so on-site visits can be infrequent.

What it costs: Managed services are priced per device or per user, per month. Prices can be anywhere between \$50 and \$200/month per device/user (with support of network infrastructure often priced differently). Sometimes companies are flexible about adding an extra device or two without extra charges. Devices include desktops, laptops, tablets, smartphones, printers, and network/server infrastructure.

Contracts generally include response time guarantees and help desk hours of operation.

Note that monthly fees do not include any project work such as systems upgrades, data migrations, etc. Projects are either billed by the hour or on a flat fee depending on provider. Equipment is not included.

Pros and cons: Monthly fees can add up quickly, making managed services expensive in many contexts. However, fees are predictable—the same amount per month no matter how much support you need—and your organization is protected from a big bill in the wake of a major problem. In addition, your interests are aligned with that of your vendor: It's better for both of you if you don't need to call them very often. This means that maintenance tends to get more attention.

Break-fix support from a support firm or consultant

What it looks like: You put in a ticket when something is wrong, and your provider fixes it in response to that request. Ongoing maintenance can also be provided on an agreed-upon schedule. Contracts can include response time guarantees and help desk hours of operation, depending on the size of the provider (a sole proprietor is unlikely to be able to offer guarantees).

What it costs: Hourly support as needed can range from \$50/hour for an independent provider with relatively little experience to \$125/hour for tier 1 (first-line) support at a high-end consulting firm, with up to \$200/hour if tier 2 (more advanced or specialized) support is needed. Many independent providers and small firms have rates in the \$75-\$100 range. Projects are generally billed at the standard hourly rate. Equipment is not included.

Pros and cons: Realistically, people use their hourly support only when problems occur so this is

always the "cheapest" (as long as things don't go terribly wrong)—and thus the riskiest, as things can and do go wrong.

Break-fix support from a device or application vendor

What it looks like: You call a hotline and/or take your device to a store when there is something wrong with it (for example, [AppleCare](#) or [Geek Squad](#)). This is generally not recommended as a sole source of support (see pros and cons), but it is often used in conjunction with other support as it can also include an extended warranty on your equipment, and even on its own it may be the best option for very small organizations.

What it costs: You generally pay a flat fee for a warranty under this system, though pay-per-incident support can be available.

Pros and cons: Coverage is generally limited and you often need to spend quite a bit of time getting service. However, covered hardware repairs can be made for no extra cost.

How to estimate your needs

A good heuristic for break-fix support is to budget 1 hour per week per staff member, assuming a your network environment is straightforward and not specialized.

If hiring internal support (a yardstick, not a recommendation!) an organization of around 7 staff likely needs 16-20 hours a week of help (per the The 2014 Nonprofit Technology Network [NTEN] staffing survey at http://www.nten.org/NTEN_images/reports/staffing_report2014_final1.pdf) A junior support person in a non-profit costs around \$40K FTE equivalent so that would be \$16K-\$20K + overhead for taxes and benefits. Maybe a little cheaper but for less expertise.

The NTEN survey has some good overall metrics on spending and staffing, as well, especially on pages 14 and 15 (non-salary overall tech spending per staff member and as percentage of operating budget).

How to choose a support provider

Choosing a tech support provider can feel like a challenge for staff who don't feel they have technical knowledge. However, you don't have to be a technical expert to find the right provider for your organization. In general, this task is best approached the same way you do when looking for any kind of vendor/partner. The steps are:

- Ask around for recommendations. Check in with your partner, ally, and peer organizations, with special attention to those that are approximately your size. Post the question on any relevant email lists or online communities you participate in.
- Contact the recommended providers and tell them you're looking for a quote for IT support. Include information about your technical landscape (what kinds of computers your office uses, what servers or other networking equipment is set up (if you know), the software people use to do most of their work, how many people they would be supporting, and how many office sites are involved). Don't worry too much about covering every single thing—they will ask you questions.

Section 7: Must Read Resources, Websites and Email Addresses

- Collect responses, follow up as needed, ask a lot of questions, ask for references (and check them!), assess, discuss internally, and decide. You will surely have several conversations with candidates. Use all of your communications to assess the fit for your organization. Things to think about:
 - Are they able to answer any and all questions clearly, without condescension and in language appropriate for a non-technical person? This is a crucial skill for tech support providers and your sales experience often gives you important insight into what the experience of receiving support will be like.
 - Do they respond to calls and emails on a timeline that feels reasonable for you? A sales process and a support process are not the same, but this is nonetheless a good metric to assess.
 - Are the pros and cons that you can see in your interactions and in their references the right tradeoffs for your organization? It's unlikely that you'll find the perfect provider for your structure and budget (for example, may not be able to afford a guaranteed 1-hour turnaround time and after-hours support), but you can choose the best fit for your organization by assessing what really matters for your specific situation.

<https://ieco.org> | 510-479-9779 | info@ieco.org