vision change win

COMMUNITY SAFETY RECOMMENDATIONS FOR FUNDERS & PHILANTHROPIC ORGANIZATIONS

May 2025 Report

INTRODUCTION

In the past year alone, we have experienced mounting political repression, state violence, and rollbacks on human rights - the unique confluence of which is unlike anything we have seen in recent movement history. The systemic targeting of Trans Communities has forced many to go without gender affirming medical care while facing increased hate and violence. Black Communities continue to face state violence in alarming numbers. We have seen statewide, and in some places region wide abortion bans and severe restrictions to bodily autonomy. Campus protests in solidarity with a free and liberated Palestine have been met with state violence, detentions, and in some cases, deportations. The war against Migrant Communities has unleashed a flood of ICE raids, unlawful deportations of both undocumented people and US citizens, and increased intimidation. The climate justice movement led by Indigenous movement leaders has experienced extreme losses both in the courts and on sacred land. Many of these threats are not new.

Drawing on movement historical lessons, the wisdom of movement elders, and our own experiences will be key to our collective survival. Despite glimpses of familiar tactics, this particular convergence of safety threats is unparalleled. And as such, this political moment is critical. For many marginalized communities, the movement wins and losses in the coming years will mean the difference between life and death. The choices we make now will have deep ripples, impacting future organizers for generations. In this critical moment of rising authoritarianism and increased attacks on movement organizations, campaigns, and leaders, philanthropic organizations have a unique and vital role.

There is a growing need for funders to recommit to those movement groups who are at the frontlines of change, and those who we know will be most targeted: Palestinian groups, Arab groups, Muslim groups, groups in solidarity with a free and liberated Palestine, Trans-led groups, Black-led groups, Immigrant rights groups and groups serving Undocumented people, Climate Justice groups, Racial Justice groups, Reproductive Justice groups, and their allies. To most effectively flank frontline organizers, funders must also invest in fortifying internal safety and security practices

for themselves and their grantees. Rather than consistently reacting to attacks and developing safety infrastructure amid crisis, we must plan. Proactively investing in strengthening grantee and funder security practices will ensure our movements are better prepared for the coming attacks against our communities.

The movement needs a united philanthropic front grounded in safety and security culture in this crucial moment. While a diligent few have invested in building safety and security skills for years, many funders are new to safety practices. This skill gap across the philanthropic sector leaves movements vulnerable to attack. There is a lack of cohesion among philanthropy, caused in part by a lack of cross-sector coordination around safety and security protocols. To reduce vulnerabilities to threats and to close this skill gap, funders should address exposure to safety threats and protocol gaps, invest in deeper safety and security leadership development, foster stronger connection and communication about safety threats across movement sectors, and build stronger trust and intentional transparency practices with grantees.

Vision Change Win believes that movement safety infrastructure cannot wait. Building movement safety infrastructure takes time, capacity, deep coordination, buy-in, and a culture shift. Investing in safety infrastructure today ensures funders and grantees can protect against rising authoritarianism in this current political moment and for the long term. Below are recommendations and best practices for philanthropic organizations and movement funders to effectively support movement groups in this pivotal political moment while planning for long-term movement safety infrastructure.

Together, we can build a strong, unified, and powerful movement.

OVERVIEW OF VISION CHANGE WIN

About Vision Change Win

Vision Change Win is a Black-led team of Queer and Trans People of Color social justice leaders dedicated to supporting organizations in fully manifesting their missions, visions, and values. We support organizations to grow their work by deepening racial justice practices, strengthening community organizing, building organizational development, organizational sustainability, conflict transformation, and restorative and transformative justice practices, and increase community safety practices.

What is Community Safety?

Community safety and security is a holistic approach to building the collective capacity and ownership for the physical and emotional well-being of those committed to building a just world. Community safety culture is based on the value that we have the power and responsibility to keep our people safe. This work includes but is not limited to action and event security, office and organizational safety, verbal de-escalation, physical de-escalation, personal safety, transformative justice processes, community safety neighborhood strategies, bystander intervention, digital security, and cop watch.

Vision Change Win's Community Safety Approach

At VCW, we believe that BIPOC (Black, Indigenous, and People of Color) communities have created safety outside of the police and prisons for generations. We draw on a rich generational legacy of community safety initiatives. VCW's approach utilizes an intersectional, trauma-informed, anti-oppression framework. Our team is adept at assessing, addressing, and transforming organizational cultures, recognizing that power and privilege are often operating around a myriad of identities simultaneously. Our team takes the time to ensure our content is relevant, accessible, and transformative for diverse communities, organizations, and groups.

For more information visit our website at www.visionchangewin.org

Summary of recommendations for building and fortifying safety infrastructure:

- [ ] Build a **security culture** and practice around "need to know" information sharing. **Page 5**
- [ ] Develop a practice of **intentional information sharing.** **Page 6**
- [ ] Build clear protocols for requesting, storing, and using **sensitive information.** **Page 7**
- [ ] Distinguish between **public and private** information. **Page 9**
- [ ] **Reduce vulnerabilities** within philanthropic organizations. **Page 10**
- [ ] Develop clear protocols for **collaboration** across foundations. **Page 11**
- [ ] Maintain high standards for **consent and trust** between funders and grantees. **Page 12**

Summary of recommendations for funding organizations:

- [ ] Increase funding for **General Operations and Community Organizing.** **Page 14**
- [ ] Fund **long-term, pro-active, and holistic** security infrastructure and plans. **Page 14**
- [ ] Fund safety planning for **targeted leaders.** **Page 14**
- [ ] Invest in **crisis communications.** **Page 15**
- [ ] Fund organizations to **hire staff** who can attend to security as a key part of their job in an ongoing way. **Page 15**
- [ ] Fund **security teams**. **Page 15**

RECOMMENDATIONS FOR BUILDING AND FORTIFYING SAFETY INFRASTRUCTURE:

1 Build a security culture and practice around "need to know" information sharing.

Strong, intentional communication between funders and movement groups is key to healthy, thriving movements. When funders are well informed on the needs of their grantees, the funding landscape is adaptive, current, and responsive. Funders often request sensitive information from grantees, such as member demographics, contact information, training participant names, campaign strategies, direct action plans, and internal organizational safety vulnerabilities. If sensitive data like this were made public or shared with bad actors, the results would likely damage many movement groups. Developing a "need to know" security ethos means paring down information requests to only the most essential, necessary information. For example, when reporting on the success of a recent grantee event, do not request participants' full names and email addresses. Instead, consider requesting the names of organizations represented or the total number of attendees. A "need to know" security ethos balances the need for information with the need to protect sensitive information from falling into the wrong hands.

Recommendations

- Funders should be mindful of requesting sensitive information from grantees, whether formally in applications or reports, or informally in status call updates, during conferences, or in casual conversations. Consider what information is "need to know" and what is "want to know" information. Clarify internally and with grantees the information required for legal or compliance purposes. Only ask for the most vital information.

2 Develop a practice of intentional information sharing.

To make a profound impact, philanthropy needs collaboration and coordination across funder groups and movement sectors. This connection enables strategic pivots that meet the moment and provide the necessary information to prepare for what's ahead. The environment and conditions in which information is shared are critical to strong collaboration and to the safety of movement groups.

Funders should place the confidentiality and safety of their movement grantees first and therefore seek not to discuss their grantees informally in any setting. For example, it would be unacceptable and dangerous for a funder to share information about a grantee's internal conflict over a drink at a hotel bar during a conference because the environment lends itself towards information leakage. It would be easy for other bar patrons to overhear this conversation. Similarly, it would be unacceptable and dangerous to share sensitive information while drinking because inebriation could lead to mischaracterization of information or sharing confidential information. Lastly, when potentially sensitive information is shared in an insecure, informal location like a hotel bar, without clear agreements about confidentiality, it is considered movement gossip.[1]

Gossip in movement settings is dangerous, especially when the gossip includes potentially sensitive information.

Recommendations

- Develop information sharing practices and agreements informed by the needs of grantees. Offer regular training on these practices and a place to troubleshoot questions as they arise.
- Refrain from sharing safety threats that grantees face with anyone, including friends, colleagues, or other funders, unless you have the express consent of the grantee.
- Set transparent agreements with grantees about when and how their data may be shared with those beyond the philanthropic organization.

Reminder: The philanthropic ecosystem is connected, so each foundation's safety practices impact other funders and grantees. What one funder practices can easily influence what others practice.

1. Movement gossip happens when sensitive, sometimes unverified information about a movement group or individual is shared in an unsecure environment or platform without the consent of the group/individual and without a clear, explicit confidentiality agreement between the information sharer and the listener. Movement gossip often spreads easily and quickly, making it difficult to contain and protect sensitive information from bad actors or the state. Funders undermine the security of social justice movements by participating in movement gossip.

3 Build clear protocols for requesting, storing, and using sensitive information.

The philanthropic landscape is a tapestry rich with connections. These connections can be a point of strength, allowing for coordinated funding efforts in crisis moments and strong communication across movement sectors. But when not navigated with intention, these connections can create movement-wide vulnerabilities. If requesting sensitive information from grantees becomes necessary periodically, like member demographics or grantee safety vulnerabilities, philanthropic organizations should develop internal organizational safety structures to protect sensitive data. These safety structures should include multiple safeguards or layers of safety practices. Each layer may have gaps or imperfections, but working together, these layers create a sturdier container. When one foundation experiences a safety threat, the impact of that threat can easily spread to other funders and even to grantees. Each foundation's safety practices impact the whole.

The following digital safety practices are part of a larger data stewardship umbrella. (Data stewardship is responsibly managing the data you hold with an emphasis on reducing any potential harm that could come from your handling of information.)

Recommendations

Minimization: Before requesting or keeping any sensitive information from grantees, consider whether it's truly necessary. Reducing the amount of data you hold is a key digital security strategy.

Communication: Do not request that grantees email you sensitive information. Sensitive data should be requested via a method that ensures data is encrypted in transit (e.g., a website that uses the HTTPS/TLS protocol) and protected at its destination. Sensitive data should be accessible only to the people who need it. It should be shared on a platform with a strong password and an application or key-based second factor authentication.

Data storage: Once sensitive data has been received as described above, it should be stored in a system with the same requirements. The information should be accessible only to those who need it via a

strong password and multifactor authentication. There should be a clear timeline for deletion set by policy, and as short as possible in light of audit and IRS requirements. Consider what could be redacted if a subset of information must be kept for long periods. The information should be password protected and only available to those within the philanthropic organization who need it. Information should live in a file system or database with role-based access control. (Role-based access control means that administrators of an information system assign permissions to users based on what they need to do their jobs. For example, the Executive Director can see all staff evaluations, but other staff can only see the evaluations of people they supervise.)

Consent and transparency: Funders should let applicants and grantees know what they are storing, where their data is stored, and how long it is kept. These safety agreements can be created collaboratively as part of grant agreements at the onset of a new grant or made iteratively as grantee needs and conditions change. Grantees and especially unsuccessful applicants should also be offered the opportunity to request deletion of their data, in alignment with consentful technology guidelines.

Protocols for data requests: Funders should set transparent agreements with grantees about when and how their data may be shared with those beyond the philanthropic organization, including consideration of how funders would handle a subpoena or other legal system request for grantees' data. To best prepare and protect against sharing sensitive data, ask for only essential and needed information, practice "need to know" data requests from grantees, avoid asking for unnecessary information, and develop clear protocols about how data will be stored.

Technology competence: Philanthropic organizations should have an identified technology partner they can turn to for security improvements and advice. Training, such as security awareness training for staff, should be mandatory.

Travel and remote work: Philanthropic organizations should provide guidance to all staff about how to maintain the organization's security while traveling and working remotely. This guidance should be done in consultation with the identified technology partner, and must include clear protocols: any needed hardware, software (e.g., VPNs, remove wipe capacity in case of device loss or theft) or equipment (e.g., laptop privacy screens), training, and support.

4 Distinguish between public and private information.

One of the pillars of community safety is to balance transparency and safety. Transparency standards for foundations have changed drastically in the past decade. The desire for stronger financial accountability has created new visibility practices that seek to highlight a fuller roster of foundations' grantees, donors, board members, and more on websites, in social media, and in newsletters. Simultaneously, as transparency standards have shifted, so has the political landscape. Some funders have shifted to meet the moment, but many have not. We reviewed a sample of our current, former, and potential funders' websites. Out of the thirty we reviewed, sixteen of them still had grantee information available and fourteen did not. Threats to individual movement leaders through doxxing and online intimidation have increased. Likewise, far right think tanks have increased their targeting of social justice organizations. To meet the moment, funders should reconsider what information should be made public and what information should be kept private or semi-private. As funders consider balancing the need for increased transparency with the need to protect movement leaders and groups, they should consider the following.

Recommendations

- Use a "need to know" framework and discuss what grantee information should be shared on websites, newsletters, and social media. These conversations should happen both internally within the foundation and with grantees, with an emphasis on consent and clarity. Smaller grantee groups, groups with more visible drop-in office space, and groups who have recently experienced safety threats may be more vulnerable.
- Consider setting protocols for when transparency standards shift. For example, groups who have recently experienced safety threats or targeting may temporarily be removed from websites to avoid further targeting.
- Consider using website inquiry forms to allow the public to submit inquiries about grantees and other semi-public information. Monitor inquiries and note inquiries that may be concerning, out of place, or requesting private information.

5 Reduce vulnerabilities within philanthropic organizations.

Funders are often vulnerable to many of the same politically motivated safety threats as the broader organizational ecosystem: bad actors, phishing, doxxing, Zoom bombing, and more. Additionally, given the role of foundations (providing money), foundations are also the target of run-of-the-mill cyber bad actors. In this critical moment, funders must build a robust internal organizational safety and security infrastructure to address potential threats. Philanthropic groups should conduct regular risk assessments (at least once a year) to determine their unique risk level, develop an inventory of safety assets and resources, and develop organizational safety and security protocols.

Recommendations

Organizational safety and security protocols: Whether it is a knock on the door or a subpoena by law enforcement, suspicious surface mail, or a digital attack, all organizations need an internal incident response plan. The plan should be clearly communicated across all business units/staff/departments. There should be an incentive to report anomalies or incidents. Too often, folks believe they will get into trouble for reporting something that is out of sorts; that is counterproductive. Develop a regular training and evaluation system for all organizational safety protocols with relevant leaders, especially during leadership changes.

Individual safety planning: Funders should take measures to offer safety planning resources to individual staff and leaders within the organization who may be specifically targeted. This may include offering tools to proactively address the threat of politically motivated doxxing or online intimidation. This may also include increasing office safety policies.

6 Develop clear protocols for collaboration across foundations

As attacks on movement organizations increase, one of the most important tools funders can utilize to predict and prevent safety threats is strong communication. Developing a regular intentional pipeline for sharing information about recent attacks and safety threats can sometimes help other foundations or grantees to prepare for threats, develop more effective intervention plans, and in some cases, prevent threats from happening entirely. To develop this intentional communication pipeline, funders must develop trusted communication channels, which include designating communication platforms for especially sensitive information.

Recommendations

Develop trusted communication channels: Clarify what channels are approved for the business of the foundation. With appropriate policy guidance, staff should understand that the business of the foundation happens using foundation-owned and approved tools. A policy can create carve-outs for tactical or highly sensitive information, which can be shared using tools such as Signal/WhatsApp/Wire, etc.

Develop threat-sharing practices: Develop a regular practice of sharing safety threats or attacks with other trusted foundations. When sharing, avoid sharing internal security fabric/architecture; instead, share the threat, the intervention, and lessons learned from the intervention.

Remember: There is no one-size-fits-all. Safety infrastructure within an organization can be modeled after existing infrastructure, but customization will always be needed to meet the unique needs of each organization.

7 Maintain high standards for consent and trust between funders and grantees.

Funders hold an incredible amount of power within movements. Program officers in particular often meet with grantees regularly, collect information about grantees, including internal organizational conflict, political disagreements, and safety threats. In addition to being a hub of information within the organizational ecosystem, funders control the direction of resources for many organizations. Because of this, trust and consent between funders and grantees are imperative for the sustained future of the organizational ecosystem. To avoid ambiguity and potential abuse of power, funders should build right relationship agreements with grantees and review/develop internal protocols.

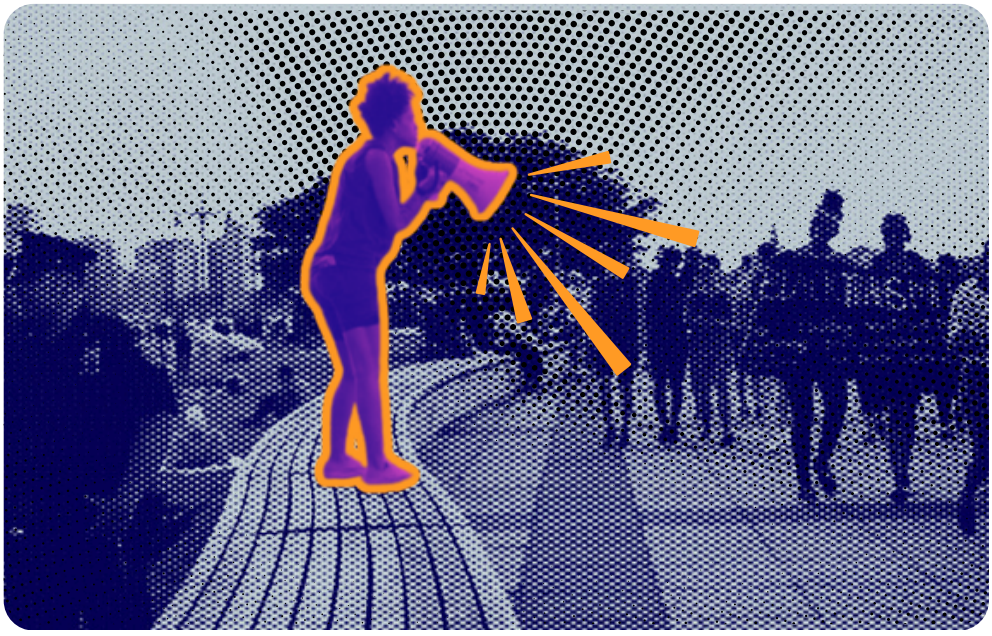
Recommendations

Develop consent agreements with grantees early and often: There is an inherent power imbalance between funders and grantees, with funders holding far more power and control over resources than grantees. This power imbalance should be acknowledged explicitly. Because of this power imbalance, developing consent agreements between funders and grantees is critical to developing healthy and trusting relationships. Consent agreements clearly name how and when a grantee may decline, or otherwise say no to a funder request. For example, if a funder requests sensitive information from a grantee outside of a "need to know" frame, a grantee should be able to easily and clearly decline the request without fear of losing grant money. This also includes consentful use of tools. For example, if a grantee is hosting a meeting with a funder and does not want a funder's AI note-taker in a meeting because of the potential for information leakage, the grantee should be clear on how and when to decline the AI note-taker from the meeting.

Develop confidentiality agreements: Grantee organizations should receive funding support and technical assistance without the fear of their sensitive information being shared broadly. Funders should develop clear and explicit agreements with grantees on what organizational information will be shared with funders and what information will not. For example, some grantees may opt not to share

with funders if there is active internal conflict being addressed within the organization. If a grantee chooses to share safety threats or attacks with a funder, then there should be confidentiality agreements set to contain the details of the threat or attack within “need to know’ communication channels only.

Develop social and sexual boundaries between philanthropic staff and grantee group leaders: Funders should develop clear internal policies for social and sexual boundaries between foundation staff and grantee leaders. When navigating platonic friendships and camaraderie between funders and grantee leaders, funders should set clear boundaries, distinguishing friendly conversation or information sharing from official business. Confidentiality and consent agreements should be upheld strictly, no matter the personal relationship a funder may have with a grantee leader. Funders should refrain from sexual relationships of any kind with leaders of grantees whom they directly fund to avoid the appearance of or actual coercion. This includes refraining from making what might appear to be sexual advances, flirting, or otherwise sexualizing interactions with grantee leaders. Under no circumstances should sexual harassment against a grantee leader be tolerated.



RECOMMENDATIONS FOR FUNDING ORGANIZATIONS:

1 Increase funding for General Operations and Community Organizing

Movement organizing work is becoming increasingly risky with new legislation, groups, and strategies targeting the movement ecosystem's ability to organize. Increasing multi-year general operating funding for organizations will increase grantees' ability to be flexible to match the shifting landscape while respecting their on-the-ground knowledge about what will serve them best.

2 Fund long-term, pro-active, holistic security infrastructure and plans

Building holistic and resilient security within social justice movements takes time, experience, and dedication. Invest in experienced organizations and institutions that support our organizational ecosystem to continue to grow our movement security capacity, ranging from threat intelligence research to rapid response support to developing curriculum, trainings, and information resources that support organizations' knowledge and skill-building. Organizations like Political Research Associates, Center for Constitutional Rights, Information Ecology, Highlander Research and Education Center, Nonviolent Peaceforce, and Vision Change Win offer movement security trainings, Know Your Rights trainings, and risk assessment trainings. In addition to the work of these organizations, fund their collaboration and information-sharing with each other and with frontline groups.

3 Fund safety planning for targeted leaders

Invest in our movement leaders, as attacks continue to target BIPOC-, Women-, Queer- and Trans- and disabled-led movements, our leaderful movements need support in addressing the targeted attacks from the far right directed at our movement leaders. This means supporting rapid response and safety planning initiatives in addition to data-scrubbing and dark web monitoring services. Safety planning may require equipment to secure homes, apartments, and offices, a security detail, or travel security. There should be funding for discovery activity as well as mitigation work.

4 Invest in Crisis Communications

When organizations or leaders are directly attacked, they often need support in quickly creating clear and effective messages for internal and external audiences about the attack. Crisis communications practitioners are essential to building effective safety infrastructure. Funders should provide rapid response grants and be sure that crisis communications costs are allowable expenses. Funders who do not provide rapid response grants should cultivate strong, trusting relationships with grantees and encourage them to reach out if they have unexpected expenses related to an urgent threat or attack. Funders may consider paying for crisis communications firms on behalf of a group, or issuing an additional grant to support the work. As always, general operating grants help ensure a non-profit can invest in proactive safety planning that will help them prepare for any potential risks or threats.

5 Fund organizations to hire staff that can attend to security as a key part of their job in an ongoing way

Organizations need at least 1-2 security-oriented staff to prioritize the organization's safety needs, ranging from providing risk assessments to the development of security protocols to ongoing training. This likely crosses many areas of organizational work and so should be integrated into different roles in alignment with what makes the most sense for each organization. The Technology Association of Grantmakers (October 2024) identified a 14:1 staff to technologist ratio. We believe a similar ratio might be a good starting point for holistic security work understanding that smaller groups will need non-staff resources to execute this work.

6 Fund Security teams

Organizations should have robust and sustainable security teams that match their organization's needs and values, so they can avoid the use of external militaristic security teams for support. In addition to the tactics named above, this looks like encouraging leaders to consider holistic security as part of all planning efforts, and offering knowledge- and skill-building opportunities to their membership.

RESOURCES

Rapid Response Support

VCW Rapid Response Support

Digital Security Resources

Five Anti-Fascist Steps for Digital Security
Doxxing Prevention Guide
Doxxing Accompaniment Guide
Digital Security Organizational Readiness Assessment Tool
Digital security foundations for organizations
Best practices for passwords and authentication practices
Best practices for Securing Your Devices

Community Safety Resources and Reports

VCW Community Safety Insights Report 2023
VCW Get in Formation Toolkit
VCW Risk Assessment Mini Toolkit
Progressive Safety Alliance website: this website contains a holistic series of political education and community safety resources.

Know Your Rights Resources:

If An Agent Knocks
Protester's Know Your Rights
Know Your Rights when protesting as a non citizen
Know Your Rights with ICE

CITATIONS

Cover Image Source: RFB PHOTOGRAFIA

vision change win