SELF-PROTECTION GUIDELINE FOR HUMAN RIGHT DEFENDERS

PREPARED BY
ETHIOPIAN HUMAN RIGHT DEFENDERS CENTER (EHRDC)

1, JANUARY 2022

Table of Contents

Preface

Ethiopian Human Rights Defenders Center (EHRDC) is a human rights organization established in December 2019 with the aim to safeguard the rights of Human Rights Defenders and ensure their safety, security, and wellbeing. EHRDC has been continuously engaging with HRDs to enhance their capacity in physical and digital security and risk management and providing protection by collaborating with different local and international stakeholders.

Through creating a safe working environment for HRDs, EHRDC intends to promote human rights and create a better world for everyone in it. EHRDC aims to enhance the capacity of human rights defenders to protect themselves and make direct interventions to provide them protection whenever their safety is endangered. This specific guideline aims to materialize the former by providing relevant protection information on how human rights defenders keep themselves physically and digitally safe.

Executive Summary

This self-guideline deliberates on protection mechanisms in place that can be utilized by human rights defenders. In particular, security mechanisms are in place. This includes measures that human rights defenders can take to pre analyze risks and prevent them and resorts in place once a threat has materialized. The guideline deliberates issues like digital security, reactionto security incidents, risk assessment and management, security plan, stress management, security at home and office,dealing with law enforcement organs during arrest and prosecutions, among others. These, together with other measures, are expected to help HRDs faced with a risk to deal with them before seeking broader help from, say, human rights organizations or lawenforcement organs.

Abbreviations

CSOs	*Civil Society Organizations*
HRD	*Human right defender*
EHRDC	*Ethiopian Human Right Defenders Center*
H.R.	*Human Rights*
NGOs	*Non-Governmental Organizations*
UDHR	*Universal Declaration of Human Rights*
U.N.	*United Nations*

Key concepts

- RISK: Risk refers to the possibility of events, however uncertain, that will result in harm.
- THREATS: Threats are indications that someone will harm somebody else's physical or moral integrity or property through purposeful and often violent action.
- VULNERABILITY: Vulnerability refers to the factors that can make it more likely that a HRD or a group will suffer an attack or will suffer greater harm because of an attack.
- CAPACITIES: Capacities are the strengths and resources a group or a HRD can access to improve their security and/or survive an attack
- SECURITY INCIDENT: Security incident is any fact or event which you think could affect your personal or organizational security

1 General Context

1. Background

As HRDs are on the frontline defending other people's rights, they often find themselves facing difficult situations such as hostile work environment, intimidation, trumped-up charges, arrest and detention, psychosocial challenges, smear campaigns, unpredictable political environment, and restrictive laws. Sometimes these risks are unavoidable; other times, they are the result of a lack of awareness of digital and physical security.

Yet, human rights defenders are key in realizing the promotion and respect of human rights as they are in constant monitoring and advocacy of human rights violations by state and non-state actors. They play a crucial role in ensuring that no one is left behind by demanding the protection of the rights of marginalized groups or individuals who are disproportionately affected. They are also essential in lessening the impact of crises such as conflict and pandemics. Human rights defenders are gatekeepers of justice and equality; hence, they must be protected. The emphasis on the situation of human rights defenders has transpired in the early 1980s as campaigns became more organized and focused. In Africa, a series of consultations had a great impact on the elaboration of the U.N. Declaration on human rights defenders. The sub-regional and Pan-African campaigns that took place in 1998 before the adoption of the declaration were clear demonstrations of NGOs' interest and commitment to defend the right to defend human rights and to campaign for a better campaigning environment for defenders throughout the continent. In subsequent movements and long years of negotiation, the need for an international instrument to recognize and protect human rights defenders was realized, and the declaration on human rights defenders was adopted by consensus by the general assembly in 1998.

Though the declaration is not a legally binding instrument, it is pivotal in the promotion and respect of human rights as it stresses the importance of human rights activists and human rights defenders. The right to be protected, the right to freedom of assembly, the right to unhindered communication with different human rights stakeholders, and the right to access a resource to protect human rights are some of the protections bestowed to human rights defenders by the declaration.

1.1. Who are Human rights defenders?

According to the 1989 United Nations Declaration on Human Rights, Defenders of human rights defenders are "individuals, groups and associations contributing to the effective elimination of all violations of human rights and fundamental freedoms of people and individuals." Human rights defenders seek the promotion and protection of all human rights for everyone and persistently hold on to human rights principles even if they operate inconvenient situations. The human rights defenders also include civil society actors who may not openly claim to be human rights defenders, such as journalists' environmental activists, development, and human rights actors. In particular, women, human rights defenders (WHRDs) are all women and girls working on any human rights issue ("women defenders" and "girl defenders"), and people of all genders who work to promote women's rights and rights related to gender equality.

1.2.Human rights defenders in Ethiopia

In Ethiopia, HRDs work under extremely difficult conditions involving threats and acts of intimidation. Though recent reform opened some space, repressive legislation in the past has had repercussions on the right to freedom of expression, association, and assembly. The challenges of HRDs in Ethiopia persist to this day, and the challenges are worsened in crisis situations such as conflict. Human rights defenders working in such areas are exposed to significant security risks because they are on the frontline of the human rights struggle and human rights violations. They are prone to intimidation and attack from both state and non-state actors. In addition, different groups of HRDs are also affected differently. For example, WHRD's consistently faced gender-specific challenges such as sexual violence and harassment. Besides, they are prone to marginalization and neglect based on their intersectional identities.

1.3. About EHRDC

After sufficient consultation held among all stakeholders and based on the needs assessment conducted by the organizing committee, the Ethiopian human rights defenders Coalition (EHRDC) was established in December 2019, after more than 60 HRDs and human rights organizations representatives met in Addis Ababa, Ethiopia at the Claiming Space forum organized by Defend Defenders (the East and Horn of Africa Human Rights Defenders Project), in collaboration with Association for Human Rights in Ethiopia, Consortium of Ethiopian Human Rights Organizations (CERO) and Ethiopian Human Rights Council (EHRCO), from 9 to 13 December 2019. EHRDC was established with the aim to have a solid national human rights defenders' network that is dedicated to protecting and defending Ethiopian human rights defenders.

2 Security Management Cycle

2. What is security management?

As stipulated in the introduction, HRD'S operate in a risk environment where they and their work could be targeted by different actors such as state and non-state actors, and it is vital for them to manage their security situation. Security management is a way of making a comprehensive security analysis and planning, including context analysis, security incidents and threats analysis, risk assessment, and security planning.

2.1. Context analysis

The work and safety of HRDs are directly and indirectly affected by the working environment, by the involvement of different stakeholders and by actors who have different characters. HRDs context analysis can be understood through three approaches.

- First is through a specific and contextualized understanding of the **Political**, **Economic, Social, Technological, Environmental, Legal, Time and other factors**. Understanding the context of each component is of high importance as those factors determine the status of HRDs and their work. *TIP: one can use the abbreviation **PESTELTO** to memorize each context*

How does this affect the risk level for human rights defenders?

- Political environment: The political environment in which HRDs operate has a direct influence on the levels of riskthey are confronted with. For example, in election periods, political tensions bring an increased risk for HRDs.
- Economic context: Economic status determines the level of protection of human rights. Also, the capacity of HRDs to put protection measures is dependent on economic capacity.
- Social context: the social context sets the tone for the work of human rights; hence is one of the major contexts to be understood.

- Technology: Technology has helped ease communication but has also created more vulnerabilities. These range from compromised channels of communication and hacking, surveillance, information theft, to shutting down digital infrastructures. Hence, HRDs are at constant digital risk.
- Environmental: Environmental context also highly affects HRDs work and safety, so it is important to study specific environmental contexts.
- Legal: Legal context in which HRDs operate is very important. The more limitations the legal framework imposes on HRDs work, the riskier the context is. On the other hand, the legal context can also facilitate the of HRDs.

2.2.Stakeholder Analysis

Identification and differentiating stakeholders are important to be able to analyze the interaction we have with stakeholders. Stakeholders can be a person, group, or organization that is interested in your work area.

Primary stakeholders: can be defenders themselves and those who work with you on a similar goal.

Duty bearer stakeholders : are actors who have a legal duty to protect HRDs (government, international bodies with mandate and armed groups to whom responsibility can be attributed).

Key Stakeholders: are actors who can influence the protection of civil society by putting pressure on duty bearer stakeholders. These can be U.N. bodies, ICRC, NGOs, religious institutions, media…

Making a stakeholder analysis is not an easy job as the involvement of stakeholders might not be static, and some stakeholders might help protect human rights defenders or be a threat for them. Hence, it is important to evaluate scenarios case by a case basis.

Stakeholder analysis in four steps:

- Identify the wider protection issue (i.e., the security situation of human rights defenders in a given region within a country).
- Who are the stakeholders? (Namely, which are the institutions and groups and individuals with responsibility or interest in protection?)
- Analyze the stakeholders' characteristics and particular attributes, such as responsibilities in protecting the power to influence the protection situation.
- Investigate and analyze relationships between stakeholders

2.3.Actors Analysis

The third is making an analysis of the actions and interests of stakeholders who can be resisting stalk holders, unknown stalk holders or supporting stakeholders. This is important to be able to have more information about them which can help make protection decisions.

3 Managing Security Incidents and Threats

3.1. What is a security incident

A security incident is any event or occurrence that can expose an HRD or organization to danger. For instance, people are sent to the offices of HRD's to find out what their routine is. They might follow up the time you start working and leave office, the communications you have, the type of transport you use. At times, an attempt of robbery or an actual robbery of the office might happen.

3.1. What is a threat

A threat is a declaration or indication with an intention to inflict damage, punish or hurt. As the work of HRDs might skirmish different actors, you are vulnerable to different types of threats. For example, it could be a direct threat that happens to you, and it is targeted towards you or an indirect threat that happens to other HRDs (e.g., closure of NGO offices is an indirect threat to other NGOs). In other cases, an incidental threat happens to you because of your appearance in the wrong place at the wrong time.

3.2. What to understand and analyze about a threat?

- It is important to look for the major facts about the treat. For instance, the profile of the person who contacts you, the time they contact you and the methods they used to contact you.
- It is also important to notice if threats are happening following your activity. For example, if the threat happens after you published a press statement or advocated for some issue.
- The other factor in giving attention to is if the threat has a pattern. For example, if you have been followed for subsequent days or if HRDs in the same area have been interrogated by authorities.
- Another important fact is the source and objective of the threat. It is very important to verify the source of the threat. For example, if it is a government authority, it is vital to ask which specific government authority? What level? What is the capacity? which personnel? what rank and so on…

Understanding the above factors is important as it will finally help you decide if you think the threat will be put into action and put security measures.

3.3. What is Risk?

Risk can be defined as the possibility of an event that can result in harm. The type of risk you face depends on the type of work you do and the specific environment you work in. Moreover, risks are not constant as they vary and change from time to time, from the environment to the environment.

3.4. What contributes to risk and risk assessment?

HRDs need to identify indicators of potential risk by analyzing the following

- The interest and approaches of different stalk holders
- The relationship between your work and the interest of those stakeholders
- Threat against defenders
- Vulnerabilities of defenders
- Capacities of defenders

3.5. What are THREATS, VULNERABILITIES AND CAPACITIES? (Risk Variables)

- **Threat:** is a declaration of intention to cause harm. Threats are generally used to make defenders feel stressed vulnerable, anxious, confused, and helpless.Defenders can face threats in different scenarios, including targeting (an attempt to change your work), common crime (if your work takes you to risky areas), and indirectthreats (can happen in conflict areas). A threat can also be declared, as in sending death threats.
- **Capacity** is any resource, including human capacity and economic resource, to improve security. For instance, knowledge of cyber security, security plan, training or teamwork can be capacities you own.
- **Vulnerability:** is any factor that facilitates harm or damage to happen. This could be weaknesses of HRDs, actions or inactions that increase the likelihood of harm occurrence or aggravate its impact. For example, lack of security locks, presence at night or lack of team support.

3.6. How to reduce risks?

To reduce risk, an HRD must reduce vulnerabilities and threats while maximizing capacities.

$$\text{Risk} = \frac{\text{Threats} \times \text{Vulnerabilities}}{\text{Capacities}}$$

4 Security Planning

4. How to Manage Security?

There are 3 types of approaches to security management

1. **Acceptance Approach:** is a strategy aimed at winning over the favor of interested parties.
2. **Deterrence Approach:** is a measure aimed at preventing unwanted access.
3. **Transfer/Protection Approach**: is leveraging from external strengths and capacities/collective security.

4.1. How do you draft a security plan?

Key questions to ask to device a security plan?

Regarding the threat

- What are the threats around you and your work?
- How do you asses the threats? (what is the level of probability of the threats materializing)
- What are the threats based on? You? Your staff? Your families? Your beneficiaries
- If the threat materializes, what will be the consequence?

Regarding yourself

- What are my vulnerabilities related to these threats?
  - Am I working in safe space?
  - Is my office at safe space?
  - Is my digital activity safe?
  - Is the staff working in a safe situation?
- What are my capacities?
  - Do I knowledge and resource to tackle the threat? (e.g., Lawyers, digital security experts, money….
  - What can I do to prevent the threat?
  - What can I do if the threat materializes?

N.B. A security plan is all about identifying your threats, vulnerabilities and risk and designing a way of tackling them. Thus, the first step is listing out capacities and figuring out what you can do with them. For example, if you have a cyber expert, you can plan to secure all your digital activities, or you might plan to change the locks of your office and set up a fence. In some cases, you might devise a regulation of how all your staff operate, considering security issues.

The security plan should be clear and have updated information. Besides, it should be available for all members of the organization.

4.2. Implementing a security plan

Once you have a clear security plan, you must make sure that you have done the following

1. Communicate with everyone concerned: if you have a staff, everyone should be informed of the reason and the specifics of your security plan. When it is important, you can also do inductions and training for staff and everyone involved.
2. Rehearse the security measures: some security measures might take a bit of time to be internalized. Hence, it is important to ensure that unfamiliar procedures are practised and that critical measures are always remembered.
3. Enforce the measures: one of the major problems around the issue of security for HRDs is that they do not practically follow security measures. So, it is important to also consider devising ways of enforcing security measures among staff, including taking actions on those who do not follow them.
4. Review it constantly: H.R. environment is dynamic, and security situations might change over short periods of time. A measure you set for one scenario might not be applicable for another. So, it is vital to regularly check and update your security plan.

Who implements the security plan?

Security plan should be implemented at every level.

1. At the individual level: as an individual HRD, you need to implement security measures to keep yourself safe. Also, as a member of a human rights organization, you have a responsibility to implement organizational security plans to keep yourself and other members of the organization.
2. At the organizational level: the whole organization must follow and implement a security plan to keep everyone safe, and the organization should be responsible for following up the implementation of different security measures.
3. At the inter-organizational level: this is when you cooperate with other organizations, agencies, and entities.

5 Reacting to Security Incidents

5. How to react to Security incidents?

When a security incident occurs, an HRD should take a number of steps to ensure the incident is properly addressed. These steps may vary on a case-to-case basis. While carrying out an analysis of the facts, certain issues need to be taken into consideration: -who might be involved?

- where did the security incident occur?

- was there any physical injury or property damage?

- what was the probable goal of the perpetrators?

This will dictate the next step on how and when to react. At this point, you should determine the gravity of the incident in order to know whether the incident is minor or serious. And also, to decide to react or not to react

5.1. Basic Actions to take when Security incidents occur.

-- Immediate action: if the specific security incidents put you in imminent danger, you need to take immediate action if, for example, you are in a situation where someone follows you, you might need to take action to shift your direction so that the perpetrator is not aware of your address.

-- Documenting: a record of security incidents should be kept in written form to prevent the loss of reported facts and to be able to record trends in security situations. The more evidence of the security incidents you have, the more it is convenient to deal with your case.

5.2.Incident Reporting

When an HRD experience or observes a security incident, an immediate report should be sent tothe designated security contact person at his/her organization or organization's managing director. To report security cases to EHRDC and to submit a protection request, you can use the following email: centerehrd@gmail.com

The following information's should be informed to the protection officer handling your case

- Who is reporting? (your organization, your personal status…)
- What happened? (explain the specific incident that happened)
- Where did it happen? (explain the setup in which the incident happened)
- When did it happen? (precisely the date and, if possible specific time in which the incident happened
- Who was involved? (what are the details of the victims of the incident and the details of perpetrators, including numbers, affiliations post-incident issues)
- What the impact is on those affected (details of their current condition and level of threat. And a summary of the current situation)
- What are you requesting from the protection department?

6 Digital Security in Communications

6. Introduction

Though access to technology and the internet is still an unresolved issue in developing countries, it has become a big part of our work at this time. Human rights organizations and human right defenders make use of technologies like the computer and the internet to improve the efficiency of their work and widen their access to information. However, the use of computers, phones and the internet come with issues like the security of data and information. As human right defenders we need to operate in a highly secured digital environment. This is crucial as the nature of human right defender's work demands a high level of security and confidentiality. In the digital world different malicious corporations, individuals and even the government might have interest to control and use information for different purposes. Hence, the digital world affected by hacking, viruses, and different intrusions.

6.1. Security when using technology

The insecurity of information does not necessarily happen through the internet, information can leak when you use technology without caution. For instance, information might leak when talking on phone or if you do not keep your files in a safe place. Hence it is important to be cautious of the following activities.

6.1. Phone communications

When talking on phone bear in mind that you are in a safe environment and you are talking to the right person. Assume that someone might be listening to you and take the necessary caution especially when you deal with a confidential information. It is also important to check your surrounding for voice recorders and similar attachments.

6.1. Storage of computer, phone, and other digital devices

- Lock computers away when leaving the office
- Turn computer screens away from the windows.
- Keep back-up information, including paper files, in a secure, separate location.
- Always shut off your computer when you leave it.

6.2. Basic internet security

- Make use of strong passwords for your devices such as your phone and computer, and also make sure the applications you use are password protected.
- Use two-factor authentication: Passwords are the first line of defence against computer hackers, but a second layer boosts protection. Many sites let you enable two-factor authentication, which boosts security because it requires you to type in a numerical code – sent to your phone or email address – in addition to your password when logging in.
- Encrypt your files in case someone does access your computer or bypasses your protection
- Keep theencrypted backups away from your office in a safe place. Erased files cannot be reconstructed if you have wiped them using PGP Wipe or another utility instead of just placing them in the computer's trash or recycle bin.
- Consider unplugging your computer's phone connection/modem or otherwise physically disabling your internet connection when leaving the machine unattended
- In your web preferences, enable file extensions in order to tell what kind of file itis before you open it. You don't want to launch a virus by opening an executablefile that you thought was text. In Internet Explorer, go to the tools menu andchoose Folder Options. Click View and make sure the box Hide extensions for known file types is NOT checked
- Viruses and other problems, such as Trojan Horses or Trojans, can come from anywhere;even friends may unknowingly spread viruses. Use a good anti-virus program and keepup to date with automatic online updating
- Confirm any suspicious requests for information by following it up through another form of communication.
- Keep your browsing activity private by not accepting cookies and by deleting your cache after every

time you use the web.

- Encrypt your email whenever possible.
- NEVER respond to spam, even to request to be taken off the list.
- Make sure the computer you are using has virus protection software.

Secure applications to use

Applications we use on our phones and computers play a big role in the security of our data and information. Some applications risk our communication and information as their buildup does not allow encryption, or the application is susceptible to being easily hacked due to its authentication method. There are some secure applications we can use to make secure communication.

6.3. Signal Private Messenger: Signal supports an extra layer of security, unlike other regular texting applications. An extra layer of security will be effective even if the other user does not use the same application. It ensures your calls in such a way that nobody can listen to them.

6.4. Secure call: provides end to end encryption for your private calls, thus preventing them from being overheard by intruders. It is an improved Android Device Manager that allows you to ring, find, lock your Android device remotely. It also allows you to wipe the device's entire data if it, by any chance it gets permanently out of your reach.

6.5. Wire: is an encrypted communication and collaboration app created by Wire Swiss. It is available for iOS, Android, Windows, macOS, Linux, and web browsers such as Firefox. Wire is one of the most secure platforms, and it can help to increase productivity by making your communication easy and secure. Messages, files, conference calls or private conversations are all supported by encryption

7 Mental Wellness/Stress Management

7. Introduction

Individuals or groups that work to protect and implement human rights often risk personal safety and mental health when defending the rights of vulnerable and marginalized groups. Usually, human rights defenders forget to give concern for their own mental health, as they work too hard, and they do not have enough time to reflect on their mental health. In such a workplace, stress is a common state of mind. **However, excessive stress can interfere with your mental health and even your productivity.**

7.1.General mental wellness Tips

- Take mental health days: we often do not give attention to our mental health being occupied with days to day hustles of life. But it is very important to take a break once in a while and give attention to our mental health.
- Talk to someone: talking to someone helps release tension and is also a good way of finding solutions to what is worrying you.
- Draw a line between your work and personal life: human rights work can be very concerning, and at times a human rights issue that you deal with at work might bother you after you go home. Hence, it is important to try and keep your personal space safe.
- Take care of your body: your physical health determines your mental health. So, make sure you eat healthily, avoid relying on substances, exercise, and get enough sleep.

7.2. Workplace Stress Management

Verywell / JR Bee

BelievePerform 2022

- **Turn to co-workers for support**: the more you share your worry with co-workers, the less your stress gets. Also, it is better to seek solutions together rather than stressing yourself.
- **Prioritizing and organizing**: often, we intend to overwhelm ourselves with lists of things to do and end up getting confused about where to start. This will lead to unnecessary stress; hence listing priority actions and organizing your schedule that way helps.
- **Create a balanced schedule**: if our schedules are not planned realistically, it might cause confusion and stress. So, it is important to set a schedule that balances your time and energy.
- **Ask for new duties**: if there is a specific task you have been working on for a long time and if you feel drained, you should work on a different task or ask for new duties
- **Delegate responsibility**: overloading yourself with sets of tasks will only be detrimental to your mental health and to your productivity. Make sure you delegate responsibilities and ask for help when you feel like you are stuck.
- **Minimize the time you spend on social media**: often, we tend to spend hours scrolling through social media and end up with no time to perform our tasks and are stressed. As HRDs, information on social media is essential for our work but limiting the time we spend on social media is vital.
- **Keep perfectionism in check:** you might be a high achiever in performing your tasks, but you cannot always do things perfectly. At times it is crucial to let perfectionism go to protect your mental health.

8. References and useful Links

8.1.References

- https://www.protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf
- https://www.verywellmind.com/how-to-deal-with-stress-at-work-3145273
- https://defenddefenders.org/
- https://quickbooks.intuit.com/r/inspiration/mentall-wellness-in-the-workplace/
- https://www.techtarget.com/searchsecurity/The-ultimate-guide-to-cybersecurity-planning-for-businesses?utm_source=google&int=off&pre=off&utm_medium=cpc&utm_term=GAW&utm_content=sy_lp01132022GOOGOTHR_GsidsSecurity_AT&T_Essential_IO159843_LI2503719=&utm_campaign=AT&T_EG_sSEC_WW=&Offer=sy_lp01132022GOOGOTHR_GsidsSecurity_AT
- https://protectdefenders.eu/protecting-defenders/
- https://www.frontlinedefenders.org/en/emergency-contact
- https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk

8.2. Useful Links

- https://pretrialrights.org/ethiopia/
- https://www.ohchr.org/EN/Issues/CivicSpace/Pages/DeclarationHumanRightsDefenders.aspx
- https://chilot.me/federal-laws/criminal-procedure-code-amharic/
- https://www.abyssinialaw.com/
- https://www.google.co.uk/url?sa=i&url=http%3A%2F%2Fwww.mirandawarning.org%2Fwhatareyourmirandarights.html&psig=AOvVaw2PScEoWi0scEmZ9AG-8_ys&ust=1643286600555000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCKil_ui1z_UCFQAAAAAdAAAAABAD