Self Protection Guidelines for Human Rights Defenders in Tanzania

TANZANIA HUMAN RIGHTS DEFENDERS COALITION

Self Protection Guidelines for Human Rights Defenders in Tanzania

COMPILED

Adv. Jones Sendodo
Adv. Deogratias Bwire

Edited by
Onesmo Olengurumwa

Contents

Preface

The Tanzania Human Rights Defenders Coalition (THRDC) is a non-partisan, human rights non-governmental organization registered under the Non-Governmental Act of 2002. The THRDC is comprised of both individual and organizational members who are currently estimated to be 150 all over Tanzania. Its membership and representation in terms of operation is spread (through designated 11 Zonal coordinating units) all over the United Republic of Tanzania (Mainland and Zanzibar).

The main interest of this coalition is to, inter alia, work towards enhanced security and protection of Human Rights Defenders (HRDs) in the United Republic of Tanzania. In accomplishing this, THRDC enhances members' self-protection mechanisms while also offering direct protection. It also intends to strengthen regional and international interventions towards protection and promotion of rights and responsibilities of HRDs.

The ultimate result of all these as this coalition visualizes is a contribution to a creation of a safer working environment for HRDs. THRDC has been and still intends to work closely with different stakeholders including local, regional and international HRDs' organizations and coalitions; individual HRDs; development partners; United Nations; duty bearers and other relevant stakeholders.

These self-protection guidelines seeks to simplify the various information that a human rights defenders need to understand for self-protection. Materials from these guidelines were gathered from different areas of which references are supplied in the last page.

Executive Summary

These self-guidelines details about various self-protection measures that a human rights defender can take to mitigate and/or prevent the risks facing them. It consists of 12 different chapters. The chapters entails issues like digital security, reaction to 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 risk to deal with them before seeking broader help from say, human rights organizations or law enforcement organs.

Abbreviations

HRDs	Human Rights Defenders
THRDC	Tanzania Human Rights Defenders Coalition
UDHR	Universal Declaration of Human Rights
NGOs	Non-Governmental Organizations
ICRC	International Committee of Red-cross
UN	United Nations
CSOs	Civil Society Organizations
Cap	Chapter
CURT	Constitution of the United Republic of Tanzania
Etc	Et cetera
HRNGOs	Human Rights Non-Government Organizations
MSA	Media Services Act
Pg	Page
TCRA	Tanzania Communication Regulatory Authority
PC	Penal Code

Chapter 1

Situational and Contextual Analysis

1.0 Introduction

The adoption of the United Nations Declaration on Human Rights Defenders in 1998 and the establishment of the mandate of the UN Special Rapporteur on the situation of human rights defenders in 2000 constitute major milestones in the protection of human rights defenders around the world. However, human rights defenders continue to face threats and risks despite the existence of these mechanisms.

Across Africa, human rights defenders working to promote and protect human rights in volatile political contexts face major risks, such as killings, physical attacks and assaults, arrests, malicious prosecution, kidnapping, state impunity, intimidation and shrinking civic space. States constantly fail to investigate violations against defenders. To ensure the security and the continuity of their work, defenders have taken steps to manage individual and organisational security by assessing risks and putting in place effective strategies to mitigate potential threats.

Dedicating time and resources to managing security helps HRDs to continue with human rights activities and ensure their safety and security. Tanzania Human Rights Defenders Coalition (THRDC) contextualised self-protection guidelines is intended to serve as a tool for human rights defenders in Tanzania to equip them with necessary strategies and responses to the often volatile environment they operate in.

1.1 The Current Situation

THRDC prepared and published Annual Situation Reports of HRDs in Tanzania from the year 2013-2017. These reports indicate that, the situation of human rights defenders in the country becomes even worse as time pass by. The most notable incidents which indicates the horrible environment HRDs are working includes, shrinking of the civic space, arbitrary arrests, malicious prosecution, HRDs being branded bad names, decriminalization of the freedom of expression, threats and attacks among others. These reports help to inform the Coalition on the best ways to tackle problems faced by HRDs and ensure their working environment is always safe. For purposes of these Guidelines situational analysis will be looked at in the following areas;

1.2 Who are Human Rights Defenders?

Human rights defenders are people who, individually or with others, act to promote or protect human rights enshrined in the United Nations Universal Declaration of Human Rights 1948 (UDHR). The 1998 United Nations Declaration on Human Rights Defenders refers to “individuals, groups and associations contributing to the effective elimination of all violations of human rights

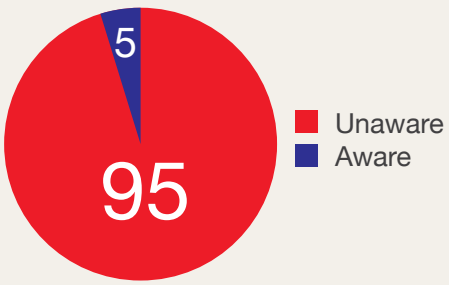
and fundamental freedoms of people and individuals." Anyone can be an HRD regardless of educational background, professional qualifications, gender, age, race, social group, or nationality. If a street vendor or a banana seller denounces the mistreatment of fellow sellers by local tax authorities, s/he is considered an HRD. In some cases, HRDs can be found in both private and government sectors. All actions taken by HRDs must be peaceful.

1.3 The Level of Awareness of Security Management and Protection Measures

According to the 2013 needs assessment report, the concept of a HRD was alien to the Tanzanian context. The roles and rights of HRDs were not very well known even to the available HRDs. Moreover, HRD knew nothing about the available mechanism for their protection whether at domestic, regional or international levels.

The report provided further that most HRDs were unaware of both physical and digital security.

About 95% of the visited human rights NGOs during the survey were unaware of security management and protection measures.



<< The pie chart left demonstrates the percentage of awareness (from a total of 200 visited HRDs) of available mechanisms for HRDs protection in Tanzania before 2013. Portion with red color represents HRDs who were unaware (95%) and the blue portion (5%) is for those HRDs found to be aware of the security and protection mechanisms.

1.4 Common Violations of Human Rights Against HRDs

The situation of HRDs over the past five years of THRDC's existence shows that human rights defenders working on pastoralist, general human rights, journalists, police, politicians have been the victims of violations. The source of the violations emanates from state impunity, existence new and old draconian laws, political atmosphere, and government regime, non-respect of the Rule of Law, strict and arbitrary enforcement of draconian laws such as the Media Services Act, 2016, Cyber Crimes Act, 2015, Police Force and Auxiliary Services Act, 1969, the Regional Administration Act, 1997 among others. THRDC normally provide support in terms of medical support, legal representation, and short term relocation and referral services to support those HRDs at risk.

The table below shows the summary of the recorded incidents to depict the Situation in numbers

YEAR	Number of Incidents recorded
2013	13 incidents
2014	31 incidents
2015	25 incidents
2016	40 incidents
2017	46 Incidents

Of the left recorded incidents many of them are with regards to malicious prosecutions, arbitrary arrests, threats, torture, decriminalization of freedom of expression, ban of newspapers, invasion of media houses, killings, and attacks among others.

Chapter

2

Making informed decisions about Security and Protection

2.0 Introduction

Understanding HRD's working environment is the key to better performance of human rights defenders work. It is therefore important for a HRD to learn different methods for undertaking context and stakeholder's analysis.

2.1 Human rights defenders' working environments

Human rights defenders usually work in complex environments, where there are many different actors, and which are influenced by deeply political decision-making processes. Many things will be happening almost simultaneously, with each event impacting on another. The dynamics of each actor, or stakeholder, in this scenario will play a significant role in that actor's relationships with others. HRDs therefore need information not only about issues directly related to their work, but also about the positions of key actors and stakeholders. HRDs should be able to organize a group brainstorming to try to identify and list all the social, political and economic actors that may have an influence on your current security situation.

2.2 Analysing your working environment

It is very important to know and understand as much as possible about the context you are working in. A good analysis of that context enables informed decisions about which security rules and procedures to apply. It is also important to think about possible future scenarios, in order, where possible, to take preventive action.

However, simply analysing your working environment isn't enough. You also need to look at how each intervention could affect the situation and how other actors might react to each one. It is also important to take into account the dimensions of a work scenario. You can undertake an analysis at macro level by studying a country or a region, but you also have to find out how those macro dynamics function in the particular area where you are working, i.e. the micro dynamics. For instance, paramilitaries in one local area may act differently to how you might expect following a regional or national analysis. You need to be aware of such local characteristics. It is also crucial to avoid having a fixed view of a work scenario, because situations evolve and change. They should therefore be reviewed regularly. Asking Questions, the Force Field Analysis and the Stakeholder Analysis are three useful methods for analysing your working environment:

(a) Asking questions

You can understand your working environment better simply by asking the right questions about it. This is a useful tool for generating discussions in a small group, but it will only work if the questions are formulated in a way that will make it easy to find out a solution.

Suppose, for example, that harassment by local authorities has become a problem. If you phrase the question as: "What should be done to reduce the harassment?, you may find yourselves simply looking for a remedy to a symptom, i.e. the harassment.

But if you phrase the question to point toward a solution, you may be on your way to finding a real solution. For example, if you ask: "Is our socio-political environment safe enough for doing our work?", there can be only two answers – yes or no.

If the answer is yes, you will need to formulate another question that can help you pin-point and properly understand the critical issues at stake for maintaining your safety. If, after proper consideration of all available activities, plans and resources, as well as legislation, negotiations, comparisons with other defenders in the area, etc, the answer should turn out to be no, this in itself will amount to a solution to your security problem.

(i) Using the Asking Questions method:

- Look for questions that will help you pin-point and properly understand the critical issues at stake for maintaining your safety.
- Formulate the questions in a solution-oriented way.
- Repeat this process as many times as necessary.

(ii) Some useful questions to be asked:

- Which are the key issues at stake in the socio-political and economy arena?
- Who are the key stakeholders in relation to these key issues?
- How might our work affect negatively or positively the interests of these key stakeholders?
- How might we react if we became targeted by any of these actors due to our work?
- Is our socio-political environment safe enough for doing our work?
- How have local/national authorities responded to previous work of rights defenders related to this issue?
- How have the key stakeholders responded to previous or similar work of rights defenders or others related to these issues?
- How have the media and the community responded in similar circumstances?.

(b) Force Field Analysis

Force field analysis is a technique which can help you visually identify how different forces are helping or hindering the achievement of your work objectives. It shows both supporting and resisting forces, and works on the assumption that security problems might arise from resisting forces, and that you could take advantage of some of the supporting forces. This technique can be completed by just one person, but is most effective when used by a diverse group with a clearly defined work objective and a method for accomplishing it.

Begin by drawing a horizontal arrow pointing to a box. Write a short summary of your work objective in this box. This will provide a focus for identifying supporting and resisting forces. Draw another box above the central arrow. List all potential forces which could be preventing you from achieving your work objective here. Draw a similar box, containing all potential supportive forces, underneath the arrow. Draw a final box for forces whose direction is unknown or unsure.

Chart 1: Force field analysis for assessing working environment

After completing your chart it is time to evaluate the results. Force field analysis helps you to clearly visualise the forces you are dealing with. The goal is to find ways to reduce or eliminate risk generated by resisting forces, partly through potential help from supporting forces. In terms of the forces of unknown direction, you will need to decide whether to look at them as supporting, or to monitor them continuously in order to detect signs of them becoming either resisting or supporting.

(c) Actors (or stakeholders) Analysis

Actors or stakeholder analysis is an important way of increasing the information you have available when making decisions about protection. It involves identifying and describing the different actors or stakeholders involved and their relationships, on the basis of their characteristics and interests – all in relation to a given protection issue.

A stakeholder in protection is any person, group or institution with an interest in, or involvement in, a policy outcome in the area of protection1.

(i) A stakeholder analysis is key to understanding:

- Who is a stakeholder and under what circumstances their “stake” counts.
- The relationships between stakeholders in protection, their characteristics and interests. How these will be affected by protection activities.
- Each stakeholder’s willingness to become involved in those protection activities.

(ii) We want to extend our work to a neighbouring area

- Powerful companies exploiting the resources.
- Government officials who benefit from bribery.
- One company has agreed to consider suspension of the exploitation
- Some international NGOs support our work.
- We have a lot of experience and strong local position

(iii) Stakeholders in protection can be categorised in the following way:

Primary stakeholders

In a protection context, these are the defenders themselves, and those they work with and for, because they all have a primary stake in their own protection.

Duty-bearer stakeholders, who are responsible for protecting defenders, i.e.:

- Government and state institutions (including security forces, judges, legislators, etc.)
- International bodies with a mandate that includes protection, such as some UN bodies, regional IGOs, peacekeeping forces, etc.
- In the case of opposition armed actors, they can be held accountable for not

attacking the defenders (as the civilian population they are), specially when these actors control the territory.

(d) Key stakeholders, who can significantly influence the protection of HRDs.

They may have political clout or the capacity to put pressure on duty-bearer stakeholders who do not fulfil their responsibilities (such as other governments, UN bodies, ICRC, etc), and similarly some of them may be often directly or indirectly involved in attacks and pressure against defenders (such as private corporations or the mass media or other governments also). All depends on the context and interests and strategies of each of these key stakeholders. A non-exhaustive list could include:

- UN bodies (other than mandated ones).
- The International Committee of the Red Cross (ICRC).
- Other governments and multilateral institutions (both as donors and policy-makers).
- Other armed actors.
- NGOs (either national or international).
- Churches and religious institutions.
- Private corporations.
- The mass media.

A major difficulty with establishing which strategies and actions are being undertaken by stakeholders is that the relationships between them are not clear-cut, or may even be non-existent. Many duty-bearer stakeholders, particularly governments, security forces and opposition armed forces, cause or contribute to human rights violations and a lack of protection for defenders. Some stakeholders, who would otherwise share the same protection concerns, may also have competing interests, such as among other governments, UN bodies and NGOs. These factors, along with those inherent in conflict scenarios, project a complex picture of the working environment as a whole.

There are a number of ways to do a stakeholder analysis. The following uses a straight-forward methodology, which is key to getting good results in analyses and decision making processes.

When assessing protection processes it is important to look at them with an adequate time perspective and always take into account the interests and objectives of all stakeholders involved.

(e) Analysing changing structures and processes

Stakeholders are not static actors. They relate to each other at multiple levels, creating a dense web of relationships. In terms of protection, it is important to highlight and pay attention to relationships which shape and transform people's protection needs. We can talk about structures and processes.

Structures are interrelated parts of the public sector, civil society or private bodies. We will look at them from the point of view of protection. Within the public sector, we could look at a government as a set of actors with either one unified strategy or with confronting internal strategies. For example, we could find strong discrepancies between the Ministry

of Defence and the Ministry of Foreign Affairs when discussing policies related to human rights defenders, or between the Ombudsman's office and the military. Structures can have mixed components; for example, an inter-sectoral commission (members from the government, NGOs, the UN and diplomatic corps) could be created to follow up on the protection situation of a given human rights defenders organisation.

Processes are the chains of decisions and actions taken by one or more structures with the goal of improving the protection situation of a given group. There can be legislative processes, cultural processes and policy processes. Not all processes are successful in achieving improvements in protection: On many occasions protection processes are in conflict or render each other ineffective. For example, people allegedly being protected may not accept a policy protection process led by the government, because they see it as having an implicit aim of displacing people from an area. The UN and NGOs may support people in this process.

(f) Stakeholder analysis in four steps:

1 Identify the wider protection issue (i.e. the security situation of human rights defenders in a given region within a country).

2 Who are the stakeholders? (Namely, which are the institutions and groups and individuals with a responsibility or an interest in protection?) Identify and list all stakeholders relevant to that protection issue, through brainstorms and discussions.

3 Investigate and analyse the stakeholders' characteristics and particular attributes, such as responsibilities in protection, the power to influence the protection situation, aims, strategies, legitimacy and interests (including the will to contribute to protection).

4 Investigate and analyse relationships between stakeholders.

After undertaking this analysis, you may wish to use a matrix like the following.

Place the list with all stakeholders relevant to a well-defined protection issue in a matrix (see Chart 2): Repeat the same list in the first column and along the first row. After this, you can undertake two kind of analysis:

- To analyse the attributes of each stakeholder (aims and interests, strategies, legitimacy and power), fill in the boxes in the diagonal line where each stakeholder intersects with itself:

  For example:

- You can place the aims and interests and strategies of armed opposition groups in the box "A".
- To analyse the relationships between stakeholders, fill in those boxes that define the most important relationships in relation to the protection issue, for example, the one which intersects between the army and the United Nations High Commissioner for Refugees (UNHCR), in box "B", and so on.

After filling the most relevant boxes, you will have a picture of the aims and strategies and interaction among main stakeholders in relation to a given protection issue.

Chapter 3

Assessing Risk

3.0 Introduction

Risk can be defined as the possibility of an event that results in harm. Risks can be dangers facing HRDs in their daily work. HRDs work can have a negative impact on specific actors' interests, and this can in turn put defenders at risk. It is therefore important to stress that risk is an inherent part of defenders' lives in certain countries. This puts them, their families, organizations, and the people they represent in danger.

3.1 Factors Contributing to Increasing Risk Levels for Human Rights Defenders

a. Political environment

The political environment in which HRDs operate has a direct influence on the levels of risk they are confronted with. For example, election periods in some areas of the country are characteristically tense and represent periods of heightened risk for HRDs.

b. Technology

The 21st century has seen technology evolve exponentially, which has greatly enhanced the capacity and impact of HRDs. Communication between defenders, countries, and continents has increased, but the transfer of information through digital means has also created more vulnerabilities. These range from compromised channels of communication and hacking, surveillance, information theft, to shutting down digital infrastructures. Even in cases where measures have been taken to set up secure systems, there have been instances where hackers or intruders have been able to tamper with or bypass the systems.

c. Thematic issues

Human rights work is at times seen by State and non-State actors as work intended to tarnish and interfere with the status quo. There are several thematic issues that have inevitably resulted in difficulties for the HRDs. These thematic areas include indigenous and pastoral rights, women and gender rights, civil and political rights, and extractives and environmental rights.

3.2 Risk Assessment

During risk assessment, HRDs needs to identify and assess indicators of potential risk. They are then able to determine the probability and impact of the risks linked to the threats.

The issue of risk can be broken down in the following way:

- Analyse main stakeholders' interests and strategies
- Assess impact of defenders' work on those interests and strategies
- Assess threat against defenders
- Assess vulnerabilities and capacities of defenders
- Establish Risk.

In summary, risk assessments involve examining threats, vulnerabilities, and capacities. There are various factors contributing to increasing risk levels for HRDs.

a. Threats

These are the possibility that someone will harm somebody else's physical or moral integrity or property through purposeful and often violent action. Defenders can face many different threats in a conflict scenario, including targeting, common crime and indirect threats. The most common type of threat – targeting - aims to hinder or change a group's work, or to influence the behaviour of the people involved. Targeting is usually closely related to the work done by the defenders in question, as well as to the interests and needs of the people who are opposed to the defenders' work.

b. Vulnerability

Vulnerability can be described as those weaknesses of HRDs that increase the likelihood of harm occurrence or aggravate its impact: just like the beautiful colour and sweet scent of flowers which make a flower more susceptible to insects' visits. The elements that an HRD possesses or surrounds himself with or even the actions that an HRD does or does not take could possibly expose him or her to harm.

Some illustrations on vulnerabilities;

- Vulnerability can be about location: a defender is usually more vulnerable when s/he is out on during a field visit than when s/he is at a well-known office where any attack is likely to be witnessed.
- Vulnerability can include lack of access to a phone, to safe ground transportation or to proper locks in the doors of a house. But vulnerability is also related to a lack of networks and shared responses among defenders.
- Vulnerability may also have to do with team work and fear: a defender that receives a threat may feel fear, and his/her work will be affected by fear. If s/he has no a proper way to deal with fear (somebody to talk to, a good team of colleagues, etc) chances are that s/he could makes mistakes or take poor decisions that may lead him/her to more security problems.

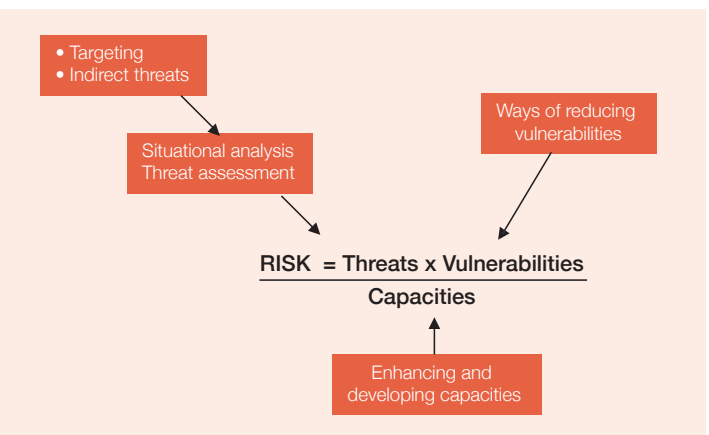
c. Capacities

Related to vulnerabilities, capacities are resources, abilities, and strengths that can be used to reduce harm and its impact: similar to using a sugar bowl with a tight lid to keep off black ants. Examples of capacities could be training in security or legal issues, a group working together as a team, access to a phone and safe transportation, to good networks of defenders, to a proper strategy for dealing with fear, etc.

Therefore;

In order to reduce risk to acceptable levels -namely, to protect- you must:

- Reduce threats.
- Reduce vulnerability factors.
- Increase protection capacities.



Risk is a dynamic concept that changes with time and with variations in the nature of threats, vulnerabilities and capacities. This means risk must be assessed periodically, especially if your working environment, threats or vulnerabilities change. For instance, vulnerabilities can increase if a change of leadership leaves a group of defenders in a weaker position than before. Risk increases dramatically with a clear and present threat. In such cases, it is not safe to try to reduce risk by increasing capacities, because that takes time.

Security measures, such as legal training or protective barriers, can reduce risk by reducing vulnerability factors. However, such measures do not confront the main source of risk, i.e. the threats, nor the will to carry them out, especially in situations where perpetrators know they are likely to go unpunished. All major interventions in protection should therefore aim to reduce threats, in addition to reducing vulnerability and enhancing capacity.

Illustration

A small group of defenders are working on land property issues in a town. When their work starts affecting the local land owner's interests they receive a clear death threat. If you apply the risk equation to their security situation, you'll realize that the risk these defenders face is very high, above all due to the death threat. If you want to reduce that risk it is probably not the moment to start changing the locks on the door of their office (because the risk is not related to a break-in at the office), nor the moment to buy a cell phone for each defender (even if communication might be important to security it is unlikely to be enough if there is someone coming to kill you). In this case, a more relevant strategy would be to work on networking and generating political responses to directly confront the threat (and if that is unlikely to be effective quickly the only way to reduce the risk significantly might be to reduce the defenders exposure, perhaps by moving away for a while – being able to relocate to a safe place is also a capacity).

Making and implementing such a decision also involves a psychosocial capacity for the defender to see that withdrawal is not a synonym of cowardice or defeat… Withdrawing can allow reflection and resuming work once better equipped.

3.3 Common mistakes about risk management

- Focus on reactive strategies: Most HRDs only put in place security management measures after facing risks or threats. The assessment of those probable risks helps to reduce their impact on HRDs and their work. Thanks to the assessment, HRDs can devise strategies to prevent such risks and to handle them in secure way.
- Copy and paste approach: Some HRDs apply security management measures that work well for other defenders. HRDs work on different themes and operate in different contexts, hence the contextualization of security measures. For example, the installation of CCTV cameras may attract attention and suspicion to HRDs working in rural areas.
- Heroism: Extreme bravery sometimes places HRDs at unnecessary risk. It is advisable for HRDs to measure their vulnerabilities vis-a-vis the magnitude of threats facing them.
- Misrepresentations of HRDs' work: In some cases, HRDs confuse political activism and human rights work, which can hinder the dialogue between authorities and civil society. Limited constructive dialogues create mutual suspicion yet governments and HRDs should work in complementarity
- Tendency to ignore one's security: in some instances, HRDs tend to give more priority to their work and victims of violations. The foundation of HRDs' work is based on their security and without it human rights work cannot be maintained.

Chapter

4 Understanding and Assessing Threats

4.0 Introduction

A threat can be defined as a "declaration or indication of an intention to inflict damage, punish or hurt." Threats are widely used to make defenders feel vulnerable, anxious, confused and helpless. Human rights defenders receive threats because of the impact their work is having, and most threats have a clear objective to either stop what the defender is doing or to force him or her to do something.

Threats represent the possibility that someone will harm somebody else's physical or moral integrity or property through purposeful and often violent action. Defenders can face many different threats in a conflict scenario, including targeting, common crime and indirect threats.

The most common types of threats are as follows;

- Targeting – aims to hinder or change a group's work or to influence the behavior of the people involved. Targeting is usually closely related to the work done by the defenders in question, as well as to the interests and needs of the people who are opposed to the defenders' work.
- The threat of common criminal attacks; this is especially if their work brings them to risky areas. Many cases of targeting are carried out under the guise of being 'ordinary' criminal incidents.
- Indirect threats arise from the potential harm caused by fighting in armed conflicts, such as "being in the wrong place at the wrong time". This applies specially to defenders working in areas with armed conflict.
- Declared threats, for example by receiving a death threat.

4.1 Components of a Threat

- A source, i.e. the person or group who has been affected by the defender's work and articulates the threat.
- Objective which is linked to the impact of the defender's work, and
- A means of expression, i.e. how it becomes known to the defender.

Threats are tricky. We might say with a certain amount of irony that threats are “ecological”, because they aim to achieve major results with a minimum investment of energy. A person making a threat has chosen to do that, rather than take action - a higher investment of energy. Why? There may be a number of reasons why, and it is worth mentioning them here:

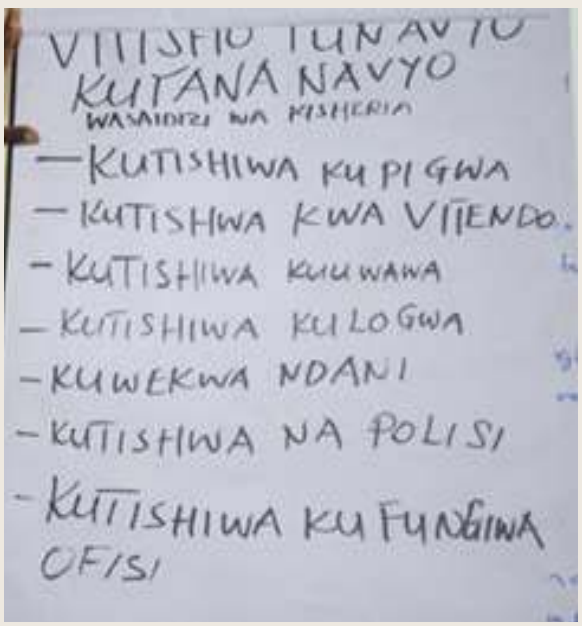
- The person making the threat has the capacity to act but is to some extent concerned about the political cost of acting openly against a human rights defender. Anonymous threats can be issued for the same reason.
- The person making the threat has a limited capacity to act and intends to achieve the same aim by hiding his or her lack of capacity behind a threat. This limited capacity may only be temporary due to other priorities, or permanent, but in both cases things may change and lead to direct action against the defender later on.

4.2 Threats and HRDs in Tanzania

Like other HRDs elsewhere, Tanzania HRDs also face threats. Threats by authorities to deregister NGOs have always been there especially to HRDs working on pastoralist issues in Loliondo (NGONET and PINGOs Forum). In 2017, there emerged threats to deregister the law society; Tanganyika Law Society (TLS) allegedly for involvement in ‘political activism’.

In a speech on 22nd June 2017, President Magufuli spoke out against education for adolescent girls who become mothers thereby expressing his disapproval of NGOs condemning the government’s violation of child rights to education.

The President stated that “as long as I’m president, no pregnant students will be allowed to return to school”. Three days later, at the Dodoma rally, Home Affairs Minister Nchemba also threatened organizations that challenge this educational ban as stated by the President with possible deregistration. Later, Association of women lawyers (TAWLA) was warned for leading other CSOs on the same issue of pregnant school girl education.



Some threats which HRDs identified to be facing during group presentation of one of the THRDC security management training sessions to HRDs.

4.3 Threat Assessment

At the end of the day, one needs to know whether the threat can be put into action. If you are reasonably sure that this is unlikely, your approach will be completely different than if you think a threat has some basis in reality.

The two main objectives when assessing a threat are:

- To get as much information as possible about the purpose and source of the threat (both will be linked to the impact of your work).
- To reach a reasonable conclusion about whether the threat will be acted on or not.

1.1.1 Five steps to assessing a threat

i. Establish the facts surrounding the threat(s).

It's important to know exactly what has happened. This can be done through interviews or by asking questions to key people, and occasionally through relevant reports.

ii. Establish whether there is a pattern of threats over time. If several threats are made in a row (as often happens) it is important to look for patterns, such as the means used to threaten, the times when threats appear, symbols, information passed on in writing or verbally, etc. It is not always possible to establish such patterns, but they are important for making a proper threat assessment.

iii. Establish the objective of the threat. As a threat usually has a clear objective linked to the impact of your work, following the thread of this impact may help you establish what the threat is intended to achieve.

iv. Establish who is making the threat. (This can only be done by going through the first three steps first.) Try to be as specific as possible. For example, you could say that "the government" is threatening you. But since any government is a complex actor, it is more useful to find out which part of the government may be behind the threats. Actors such as "security forces" and "guerrilla groups" are also complex actors. Remember that even a signed threat could be false. This can be a useful way for the person making the threats to avoid political costs and still achieve the aim of provoking fear in a defender and trying to prevent him or her, from working.

v. Make a reasonable conclusion about whether or not the threat can be put into action. Violence is conditional. You can never be completely sure that a threat will – or will never - be carried out. Making predictions about violence is about stating that, given certain circumstances, a specific risk exists that a particular person or group will act violently against a particular target.

Chapter 5

Security Incidents

5.0 Introduction

A security incident is any event that can expose HRDs and/or their organizations to danger. Security incidents provide lessons to HRDs and their organizations on the impact of their work and how various people's interests are affected. They also give opportunity to HRDs and their organizations to re-assess their security and protection mechanisms.

Examples of security incidents:

- In some cases, people are sent to the offices of HRDs to find out when HRDs come and leave their office, the means of transport they use, the colour of their car, etc.
- Leakage of information on sensitive cases can cause security threats such as detention, stalking and intimidation from anyone implicated in the human rights violations;
- If visitors are not well screened and their identities documented, anyone can enter the offices of HRDs and commit a crime or compromise their security. They can go even unpunished because there is no record of their visits.

'A security incident represents "the minimum unit" of security measurement and indicates the resistance/pressure on your work. Do not let them go unnoticed'!

5.1 The situation of HRDs in Tanzania

As will be explained below, recognizing security incidences needs some kind of awareness on security and protection to HRDs. Normally, many HRDs who are not conversant with security and protection rules take security incidents for granted and they do not analyse them.

In Tanzania for example, during the establishment of the THRDC, very few HRDs were knowledgeable of security and protection issues. According to the 2013 THRDC needs assessment survey, only 135 out of 2000 projected individuals HRDs in human rights organizations and the media had attended security management trainings whether in the country or outside Tanzania.

The inception of THRDC particularly the capacity building and empowerment program, has opened eyes of many trained HRDs in matters of security and been able to recognize the nature of their working environment hence easy to note and identify and respond to security incidents whenever they are targeted.[1]

To illustrate this, here are some noticed security incidences by trained HRDs which were reported to the Coalition;

- Mr. Deus Kibamba (Former Executive Director, Jukwaa la Katiba/Constitutional Forum)

  On 12nd April 2013 around 11 a.m. to 12 p.m. a dark blue Land cruiser with registration number T 126 CCG, was seen packed at the CF premises with six men, two of whom went to the main gate of this office and requested for the CF's Chairperson Mr. Deus Kibamba and its coordinator, Ms. Diana Kidala. The duo pretended to have been related to Mr.Kibamba. Ironically, they requested for his phone numbers after they realized that they had hit a snag. The duo was reported to have stayed outside the CF's offices for about an hour apparently in a serious discussion. CF reported the matter to the Police while THRDC issued a press statement and there after took over the case by conducting a serious investigation.

- Mr. Antony Lyamuda, Executive Director Civil education is the Solution for poverty and Environmental Management (CESOPE)

  On March 2013 Lyamunda was threatened several times by unknown assailants. He was then subjected to constant surveillance. Reacting to these security incidents he was assisted to fly out of the country for security reasons.

- Mr. Maxence Melo, the Executive Director, Jamii Media (JamiiForums) as one of the websites provides an access to users to post, engage and follow up posts of various issues and information of various matters regarding the society). He reported several security incidents and threats to the Coalition which included over five demand letters issued to him in 2016 by the police compelling him to reveal the IP address its users at Jamii forums platforms. Police invoked section 32 of the Cybercrime Act.

- Onesmo Olengurumwa's, National Coordinator-THRDC was in 2017 and 2018 interrogated several times about his nationality due to his human rights work. He was arrested and prosecuted in 2017 during the launch of a book of a young HRD, Alphonce Lusako. Unknown people had been vividly seen in his home while he is away asking the kids about the whereabouts of their farther.

5.2 How to React to Security Incidents

The impact of an HRD's work can often be gauged by the reaction HRDs receive from their community. When a security incident occurs, a HRD should take a number of steps to ensure the incident is properly addressed. These steps may vary on a case-to-case basis.

Step 1: Incident Reporting

When an HRD experiences or observes a security incident, an immediate report should be sent to the designated security contact person at his/her organisation or organisation's managing director. THRDC members can directly inform the THRDC's protection officer at THRDC's headquarters.

Key information in this report should include:

- Who is reporting?
- What happened? Where did it happen? When did it happen, as precisely as possible);
- Who was involved, what are the details of the victims of the incident?
- What the impact is on those affected, with details of their current condition;
- Who perpetrated the incident, with brief details of numbers, weaponry, apparent affiliation, post-incident actions;
- Summary of the current situation and whether there are problems or not;
- If yes, what decisions and actions that the rapporteur proposes to take/has taken and what actions requested.

Note: Incident reporting can be written or verbal. However a record of the incident should be kept in written form to prevent the loss of reported facts.

Step 2: Analyze the facts

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 damaged, 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.

Step 3: To react or not to react

When the analysis shows that the security incident is serious, HRDs should take necessary actions. The actions depend on the nature of the security incident. In case of an office break-in, new locks and security systems should be put in place. If a security incident is considered as minor, HRDs may not react but they are required to document the incident for future reference.

Chapter 6

Preventing and Reacting to Attacks

6.1 Introduction

Attacking is a process, as well as an act. Careful analysis of attacks often shows that they are the culmination of conflicts, disputes, threats and mistakes which have developed and can be traced over time.

Attacks against HRDs are the product of at least three interacting factors:

- The individual attacker. Attacks on HRDs are often the product of processes of thought and behaviour we can understand and learn from even if they are illegitimate. The party will need to invest means at least to gather information (security incidents) about the target HRD.
- Background and triggers which lead the attacker to see the attack as an option. Most people who attack HRDs see attacking as a way of reaching a goal or 'solving a problem'.
- A setting that facilitates the attack.

6.2 The brief situation in Tanzania on the attack of HRDs

Unlike previous years, Tanzania has recently started to witness growing trends of attacks, disappearances and kidnapping of HRDs and journalists by unknown assailants. The trend of interruption of HRDs internal meeting and arbitrary arrests has been rampant.

In all the five years that THRDC has been operating, journalists, police officers and other HRDs have been the victims of attacks. In 2017 for example three law offices (law firms) were invaded and one among these (IMMMA Advocates) was bombed causing a huge property loss and fear within legal profession. In September 2017 there was a shocking attack to HRDs and the then Tanganyika Law Society President, Hon. TunduLissu. Attackers of the above named HRDs have never been identified, caught and arraigned to court to face their appropriate charges.

6.3 Who is a Danger to HRDS?

Generally, anyone who thinks that attacking a HRD is a desirable or a potentially effective way to achieve a goal.

6.4 Surveillance and Counter-Surveillance

Some attacks are preceded by threats. Others are not. However, the behavior of individuals planning a targeted violent attack often shows subtle signs, since they need to gather information about the right time to aggress, plan how to get to their target, and how to escape.

Surveillance of HRDs usually takes place at their workplace, homes or places where they socialize. Attacks are carried out at HRDs' moments of greatest vulnerability and weakest capacity. Anyone in your area, such as doormen or porters in buildings, travelling sales people who work close to the building entrance, people in nearby vehicles, visitors, etc., could potentially all be watching your movements.

Surveillance can be used for a number of purposes

- To establish what activities are carried out, when and with/by whom.
- To use this information later to attack individuals or organizations.
- To gather the information necessary to carry out an attack.
- To gather information for legal action or other harassment (without direct violence).
- To intimidate you, your supporters or other people who work with you

It is therefore vital to detect and analyze any signs indicating a possible attack (counter surveillance). This involves:

- Subtly watching those who could be watching you
- Noticing movements of people in your area and changes in their attitude
- Involving a trusted third party to watch them for you without confronting them or letting them know
- Before arriving home you can ask a family member or trusted neighbour to take up a position close by (e.g. changing a car wheel), to check if somebody is awaiting your arrival
- Identifying and analysing security incidents
- Determining the likelihood of a threat being carried out

It is important to note that;

- Attacking a defender isn't easy and requires resources.

  Surveillance is needed to establish an individual's movements and the best location for attacking. Getting to the target and making an effective, quick escape is also vital. (However, if the environment is highly favorable to the attacker, attacks are easier to carry out.)

- People who attack defenders usually show a degree of consistency.

  The majority of attacks are aimed at defenders who are heavily involved in issues affecting the attack. In other words, aggressions are not usually random or aimless, but respond to the interests of the attackers.

- Geographical factors matter.

  For example, attacks on defenders in rural areas may be less public and therefore provoke less reaction at law enforcement level and political level than attacks in urban areas. Attacks against NGO headquarters or high profile organizations in urban areas generate a greater reaction.

- Choices and decisions are made before an attack.

  People who are considering an attack against a defenders' organization must decide whether to attack the leaders or grassroots members, and choose between a single hit (against a key, possibly high- profile person and therefore at an increased political cost for the attackers) or a series of attack (affecting the organization's membership). The few studies done on attacks against defenders suggest that both strategies are usually applied.

Chapter 7

Arrest, Detention and Prosecution of a Defender

7.0 Introduction

It is important to note that, arrest, detention and prosecution of a defender or any other person is governed by different laws with different law enforcement organs being involved. Therefore, a HRD need to be conversant albeit in brief about his/her rights while any of the above incidents are involved.

7.1 Brief situation of arrests, detention and prosecution of a defender

The situation of arrests, detention and prosecution of human rights defenders in Tanzania has become rampant over the past two years. This is mainly because of the arbitrary use of powers, state impunity, political atmosphere, non-respect of the rule of law and good governance. Human rights defenders have been the most affected group in these incidents. Tanzania Human Rights Defenders under its Protection Desk for the year 2016 and 2017 was able to record more than 70 incidents of violations of human rights including arbitrary arrests, unlawful detention, and malicious prosecution. These incidents not only violate the rights that human rights defenders are inherently endowed with but also make their working environment even worse.

7.1.1 Arrest

The act of arresting a person has been associated with a variety of disturbing forms of conduct. There are times when the police use excessive force when affecting an arrest, even when the suspect has clearly expressed willingness to go to the police station without being handcuffed. It seems ingrained in the minds of the police that the first step in dealing with a suspect is to degrade and humiliate him or her before relatives and friends. The law does not direct the police to behave in such an unruly manner.

The first step that the law directs is merely the arrest of the suspect. More often than not, once a person is told that he or she is under arrest and informed of the probable reasons therefore, he or she would promptly oblige. It is only in cases where the suspect does not oblige that the police are permitted to touch the body of the person or handcuff him/her. If the suspect refuses to be arrested, then the police are allowed to use reasonable force to effect the arrest. It must be emphasized that a suspect is entitled to be informed of the offense of which he or she is suspected and for which he or she is being arrested.

When the police arrest someone, they take away that person's fundamental right to freedom. Consequently, there are several procedures the police must follow before they can make a legal arrest so that human rights remains protected.

According to the Criminal Procedure Code, 1985, arrested person has got several rights to be complied with. Arresting officer should therefore ensure he/she complies with the arresting procedures.

(a) When may an officer arrest someone?

There are only a very limited number of circumstances in which an officer may make an arrest.

- The officer personally observed a crime;
- The officer has probable cause to believe that person arrested committed a crime;
- The officer has an arrest warrant issued by a magistrate.

(b) Procedures of Arrest

The rules regarding what an officer must do while making an arrest in Tanzania is provided for under the Criminal Procedure Act, 1985. Generally, an arrest happens when the person being arrested reasonably believes that she is not free to leave. The officer need not use handcuffs, or place the arrestee in a police cruiser, although police often use these tactics to protect themselves. Police also do not have to read the Criminal Procedure Act, 1985 at the time of arrest.

However, the police must read to a suspect his/her rights under the Criminal Procedure Act, 1985 before an interrogation, so many police departments recommend that the Rights of suspects be read at the time of arrest. This way, they can start questioning right away, and also, any information volunteered by a suspect can be used against them. Finally, although police will almost always tell an arrestee why they are under arrest, they may not necessarily have any legal obligation to do so.

One universal rule police officers must follow is that they are not allowed to use excessive force or treat the arrestee cruelly. This is also provided for under the Police Force and Auxiliary Services Act, 1969. Generally, police officers are only allowed to use the minimum amount of force necessary to protect themselves and bring the suspect into police custody. This is why people are advised to never resist an arrest or argue with police. The more a suspect struggles, the more force is required for the police to do their job. If the arrestee thinks the arrest is unjustified or incorrect, he/she can always challenge it later with the help of a lawyer, and if warranted, bring a civil rights case.

(c) Search

Search must be carried in accordance with the law and laid procedures, because it interfere ones privacy, liberty and freedom as are provided in the Constitution. Hence you must seek search warrant from appropriate authority.

Two types of search;

- First is warranty from in charge of a police station. This may be issued to any person including police officers.
- The second one is search warrants by the court.

1.1.2 Detention

It should be noted that, detention of a HRD or any other person curtails one's liberty according to the Constitution of the United Republic of Tanzania. This is why detention of a person has time limit. The maximum time limit provided by the law is 24 hours of which the arrested person is supposed to either be taken to court or granted police bail.

In the circumstances where a HRDs/any other person stays in police custody or any other detention facilities without any of the above being done, it advised that an application for bail and/or habeas corpus be filed in courts of law to request the court order that the said HRD be brought to court to face the charges appropriate to him/her. In making applications of this nature, a HRD needs to get the assistance of the advocate and in this regard, THRDC can intervene and assist.

1.1.3 Prosecution

It is important to note that, one of the protection services offered by THRDC is legal representation. Therefore HRDs faced with legal challenges are immediately supposed to report the same to THRDC for further assistance. However, we guide a HRD to understand the ABCs of prosecution as a self-protection strategy. In this part a HRD shall be referred to as the accused. Prosecution is normally conducted in compliance with the following;

(a) Charge Sheet (Charge)

Charge is a foundation of institution of criminal proceedings against an accused. This is a document that states the offences and provisions of the laws that the accused has breached, together with his personal information. Prosecution will draw charge if the case is triable by subordinate courts or information if the offences are triable only by High Court. There are certain offences triable by High Court only such as incest, murder, arson and treason.

(b) Plea Taking

Here the accused will be required to plead for the charges read to him/her .The accused will be asked by the court to give a plea of guilty or not guilty. If the accused plead guilty the plea must be unequivocal, which means clear plea if the plea is not clear court enters a plea of not guilty. If plea of not guilty is entered by the court the prosecution will be allowed to proceed to present their case. If postponed the accused will have a chance to ask for bail, if is bailable offence. If the plea of guilty is entered then the procedure will skip to Acquit/Convict till the end.

(c) Court Bail

Most of time if accused plead guilty and plea is entered bail do not apply. After plea a person is remanded or bailed. Bail is constitutional right s.13 (6) (b) of United Republic of Tanzania Constitution, [Cap 2, R.E 2002], presumption of innocence. There are unbailable offences like. Treason, armed robbery, defilement and murder under s.148 (5) of Criminal Procedure Act. Police bail can be granted before matter set to court; court bail is when the matter is set in court.

(d) Preliminary Hearing (PH)

This is an important stage where the parties meet to draft a memorandum of agreed fact so as to expedite the case speed .The parties have to meet decide on what matters are not in dispute and those matters are not supposed to be brought during trials neither party is required to prove any of those facts except the facts in dispute only.

(e) Trial Stage

This is when the case is set for hearing or mention and the prosecution have to prove whether they have case against the accused or not before the court.

- Prosecution Case

  This is a stage where the prosecution have to present their case ,where the prosecution will call upon the witnesses to give their testimonies and present any other evidence that support their case, for court to decide whether there is a case to answer or not. It is in this stage where the witness will be examined by prosecution at first (Examination in Chief), then will be examined by defense (Cross examination) lastly will be re-examined by prosecution (re-examination). Importantly: Generally the burden of proof lies on Prosecution and the standard of proof is beyond reasonable doubt.

(f) Case to Answer /No Case to answer

This is a stage where the court has to decide on whether there is a case to answer or not, basing on the evidence provided by prosecution. If no case to answer the court will acquit the accused, if there is a case to answer accused will be having chance to present evidence in his support.

(g) Defense Case

Basically here the defense team will present their evidence, witness be examined in chief, cross examined by prosecution and re-examined by the defense.Final Submission:

This is a summary of the whole presentation from each side; defense will be the first to make their final submission then followed by the prosecution side. Final submission can be orally or in writing, this have to be with the leave of the court.

(h) Acquit or Convict

This is a stage where by the court will rule depending on the submission by prosecution and defense if the accused is found guilty or not. Therefore the accused can be found not guilty, if found not guilty, game over, he will be acquitted and set free, If found guilty the next step will follow.

(i) Mitigating and Aggravating factors

When the accused is convicted, Defense will be given chance to present factors that tend to diminish the magnitude of sentence whereas prosecution will be give factors that tend to increase the magnitude of the sentence.

(j) Sentence and Judgment

This will be second last thing, the court will read the sentence in the judgment and there is a set rule in the law that it shall be within ninety days under s.311 of the Criminal Procedure Act. The contents of the judgment are provided by the law under s.312 of CPA.

(k) Right to Appeal explained

The judge /magistrate must pronounce the right to appeal for any aggrieved party with the decision. Note: The sixty days rule established under section 225 of CPA require criminal prosecution to be finalized within 60 days from the day of their commencement subject to certain exceptions like in serious offences whose investigation is likely to protracted such as treason.

Chapter

8 Improving Security at office and Home

8.0 Introduction

Security at the organisation's headquarters or offices and in staff members' homes are of paramount importance to human rights defenders' work. These guidelines will therefore go into some depth about how the security of an office or home can be analysed and improved.

8.1 General aspects of office security

The aims of improving security can be summarised in the following words:

- Prevent unauthorised access. In rare cases it is also necessary to protect an office against a possible attack (against bombing).
- The vulnerabilities of an office. These serve to increase risk, depending on the threat you are facing. For example, if you are at risk of someone stealing equipment or information, you must remove your vulnerabilities accordingly. A night alarm is of little use if nobody is going to come and check what has happened. On the other hand, if there is a violent break-in in daylight, reinforced railings on the door or alarms won't be very useful. In short, take measures according to the threats you face and the context you are working in.
- The vulnerabilities of an office must be assessed in the light of the threats you may face. However, it is important to find a balance between putting appropriate security measures in place and giving outsiders the impression that something is being "hidden" or "guarded", because this can in itself put you at risk. In office security you often have to choose between keeping a low profile or taking more obvious measures if need be.
- The security of an office is no greater than its weakest point. If somebody wants to gain entry without your knowledge, they won't choose the most difficult point of entry to do it. Remember that the easiest way of gaining access to an office and observing what goes on inside is sometimes simply to knock on the door and go inside.

8.2 The office location

Factors to consider when setting up an office are:

- The neighbourhood; whether the building is associated with any particular people or activities from the past;
- Accessibility on public and private transport;
- Risk of accidents;
- How suitable the building is for putting the necessary security measures in place, etc.

It is useful to review which security measures are being taken by others in the neighbourhood. If there are many, this may be a sign of an unsafe area, for example, in respect of common crime. It is also important to talk to people in the area about the local security situation. In any case, make sure security measures can be taken without attracting undue attention. It is also useful to get to know local people as they can pass on information regarding anything suspicious going on in the neighbourhood.

It is also important to check out who is your landlord. How is their reputation? Could they be susceptible to pressure from the authorities? Will they be comfortable with you putting security measures in place?

The choice of office must take account of who needs to come to the office. An office where victims come to seek legal advice will have different requirements to an office which is primarily a place for staff to work. It is important to take account of how easy it is to get to by public transport, will it result in unsafe journeys between the area where staff live, those where most work activities take place, etc. The surrounding areas must be evaluated, especially in order to avoid having to travel through unsafe areas.

Once the location has been selected, it is important to do periodical evaluations of aspects of the location which can vary, for example, if an 'undesirable element' moves into the neighbourhood.

Checklist For Choosing A Good Office Location

NEIGHBOURHOOD:	Crime statistics; closeness to potential targets of armed attacks, such as military or government installations; secure locations for taking refuge; other national or international organisations with whom you have a relationship.
RELATIONSHIPS:	Type of people in the neighbourhood; owner/landlord, former tenants; former uses of the building.
ACCESSIBILITY:	One or several good access routes (the more, the better); accessibility by public and private transport.
BASIC SERVICES:	Water and electricity, phone.
STREET LIGHTING	In the surrounding area.
SUSCEPTIBILITY TO ACCIDENTS OR NATURAL RISKS:	Fires, serious flooding, landslides, dumping of dangerous materials, factories with hazardous industrial processes, etc.
PHYSICAL STRUCTURE:	Solidity of structures, facility for installing security equipment, doors and windows, perimeter and protection barriers, access points (see below).
FOR VEHICLES:	A garage or at least a courtyard or enclosed space with a parking barrier.

1.3 Other important factors to be taken into consideration to improve security at home and office;

(a) Fence including electric fences. It is important that where resources allows, HRDs offices are properly fenced and where possible, these should be electric fences.

(b) Office facilities and trainings (first aid kit, fire extinguishers, regular trainings on how to use them. Use also toll free numbers.

(c) Office Keys-Should be invisible especially to intruders. Lock them in a place/safe where few people have access. Make regular changes of password of the safe/locker

(d) If you are leaving your office, even if it is for a few minutes, make sure you lock your computer and safeguard your confidential papers from easy reach of children and intruders. Make sure that your office doors and cabinet are locked, whether you are in or out of the office. Before you finally leave your office for the day, ensure you clean your desk and dispose every document. Also, make sure you lock your windows, file cabinets and desk drawers.

(e) Label Your Office Equipment. Make sure you label your office equipment with ID labels, seals or stickers with your inventory number and logo.

(f) Keep a comprehensive list of all the things in your office, in a visible place (preferably on the office wall), so that you and your co-workers can check at any time to see that everything is in its rightful place.

(g) Wear Identity Badges. Ensure all your employees have their names boldly written on their identity badges. More so, office customers or clients should be given guest identity badges. This is a great security measure you can use to your advantage. With it, you can know who is coming or going out of your office premises.

(h) Install CCTV Systems. The benefits of CCTV systems are multiple. It serves as a guide for your employees and also a way to catch intruders or criminals in your office. Installing CCTV systems is one of the easiest and most innovative ways of boosting security in your office. If you want to bolster the security of your office or workplace, make sure you install CCTV in the garage and entrance of your office.

(i) Invest in Alarm Systems. The most effective way to enhance the security of your office is by adding alarm systems. The benefit is similar to the installation of CCTV cameras in your workplace. Installing alarm systems will act as a deterrent, once people noticed the place is armed with alarms, they will be careful how they come in and go out of the place. The beauty of alarm systems is that it will alert authorities if there is any trace of criminal activity, and potential trespassers or thieves will avoid coming to your office.

(j) Keep Your Passwords Private. Ensure your identity badges, keys, computer passwords, and keycards are secure or safe. You can do this by making sure you don't give it out to someone you can't trust. If it is possible for you, ensure you don't give it out in the first place. There are people you will give it to on trust, and they will abuse the privilege by misusing them,

(k) Know your neighbourhood. Do you know your neighbours and your neighbourhood? Criminals more often than not watch property before they decide where and when to break in, check when you and your family come and go. Knowing your neighbourhood and people living around you will help you spot suspicious onlookers. Your neighbours can be a helpful first line of defence against a home invasion. They know the area and can help keep an eye on your home when you're away — but they can't do that if they don't know you. Make an effort to meet your new neighbours and form good relationships so you'll have people to rely on. If something fishy is happening in your area, a good neighbour will call and let you know. Talk to your neighbors about any suspicious people or strange cars you notice lurking about.

(l) Know your land lord. Whether the land lord will agree with you installing security measures at your office?

(m) Light up all the areas surrounding your office and home.

Chapter 9

Security in Communications and Information Technology

9.0 Introduction:

You are a 21st Century African Human Rights Defender. You are armed with your keen intellect, strong sense of social justice, connections to local communities, a mobile phone, an iPad, and a laptop. Twenty years ago you certainly would have had the first three but the phone in your pocket and the laptop in your bag are unique to the 21st century. Digital technology complicates our ability to assess our personal and professional risk because they are almost always unintuitive. Without specialist and technical knowledge it is difficult to analyse where devices betray the trust put in them to store sensitive files and communicate confidential information. With the enactment of Cyber Crimes Act, 2015, The Online Contents Regulations, 2018 which to a greater extent have restrictions on the use of online platforms such as Email, Skype, Facebook Messenger, Instagram, Twitter and Whatsapp, youtube etc, it is important to operate safely online.

9.1 Talking

Information doesn't need to pass through the internet to be illegally accessed. When discussing sensitive issues, consider the following questions:

- Do you trust the people you are talking to?
- Do they need to know the information you are giving them?
- Are you in a safe environment? Bugs or other listening devices are often specifically planted in areas where people assume they are safe, such as private offices, busy streets, home bedrooms and cars.

It may be difficult to know the answer to the third question, because microphones or bugs can be planted in a room to record or transmit everything being said there. Laser microphones can also be directed at windows from great distances to listen to what is being said inside a building. Heavy curtains provide some protection against laser bugs, as does installing double glazed windows. Some secure buildings have two sets of windows installed in offices to reduce the risk of laser listening devices.

(a) What can you do?

- Always assume someone is listening in. With an attitude of healthy paranoia, you are more likely to be careful when it comes to confidential matters.

- Bug sweepers or sniffers can detect listening devices, but can be expensive and difficult to obtain. Also, sometimes the people hired to conduct the bug sweeps are responsible for the original bugging. During a sweep, they either find a few "throwaways" (cheap bugs designed to be found) or miraculously find nothing and declare your offices "clean".

- Any cleaning staff could be a serious security threat. They have afterhours access to your offices and take all your waste away with them every night. All staff should be vetted carefully for security clearance on an ongoing basis, as staff may be compromised after they join your organisation.

- Change meeting rooms as often as possible. The more rooms or places you use to discuss and exchange information, the more manpower and equipment will have to be used to listen in.

- Beware of gifts designed to be kept with you at all times, such as an expensive pen, lapel pin or broach, or used in your office, such as a beautiful paperweight or large picture. These kinds of objects have been used in the past to listen in on conversations.

- Assume that some proportion of your information is compromised at any given time. You may wish to change plans and codes often, giving your listeners only fragments of true information. Consider giving out false information to check if anyone uses or responds to it.

- To minimise laser microphone effectiveness, discuss delicate matters in a basement or a room with no windows. Some laser listening devices can be less effective during rainstorms and other atmospheric changes.

- Play an audio recording of white noise or a popular song to interfere with sound pick-up. Only expensive technology can filter out random noise to hear a conversation.

- Wide open spaces can be both helpful and harmful. Meeting in a secluded place makes it easy to see if you're being followed or observed, but makes it difficult to escape by blending in. Crowds make it easier to blend in, but far easier to be seen and heard.

(b) Mobile phones

All phone calls can be listened into if the listener has enough technological capacity. No phone call can be assumed to be secure. Analogue mobile phones are much less secure than digital mobile phones, and both are much less secure than landlines.

Both your location and your conversations can be picked up through cellular surveillance. You don't have to be talking for your location to be tracked – this can be done anytime your mobile phone is switched on.

Do not keep information such as sensitive names and numbers in your phone's memory. If your phone is stolen, this information can be used to track down and implicate people you want to protect.

(c) Basic computer and file security

- Lock computers away when leaving the office, if possible. Turn computer screens away from the windows.
- Use surge protectors for all power outlets (variations in the electrical current can damage your computer).
- Keep back-up information, including paper files, in a secure, separate location. Make sure your back-ups are secure by keeping them on an encrypted computer hard drive with a secure data back-up organisation, or secured by sophisticated physical locks.
- To reduce the risk of someone accessing your computer, passphrase-protect your computer and always shut off your computer when you leave it.
- Encrypt your files in case someone does access your computer or bypasses your passphrase protection. If your computer is stolen or destroyed, you will still be able to recover your files if you have created a secure back-up every day. Keep the encrypted back-ups 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.
- Your computer can be programmed to send out your files or otherwise make you vulnerable without your knowledge. To avoid this, buy your computer from a trusted source, flatten the computer (i.e. reformat the hard drive) when you first get it, and then only install the software you want. Only allow trusted technicians to service your computer and watch them at all times.
- Consider unplugging your computer's phone connection/modem, or otherwise physically disabling your internet connection, when leaving the machine unattended. This way, rogue programs calling out in the middle of the night will not work. Never leave your computer on when you leave for the day. Consider installing software that will disable access after a certain set time of inactivity. This way, your machine is not vulnerable while you get a coffee or make a photocopy.
- In your web preferences, enable file extensions in order to tell what kind of file it is before you open it. You don't want to launch a virus by opening an executable file that you thought was a text file. In Internet Explorer, go to the Tools menu and choose Folder Options. Click View and make sure the box Hide extensions for known file types is NOT checked

(d) Basic internet security

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 keep up-to-date with automatic online updating. New viruses are constantly being created and discovered, so check out the Virus Information Library at www.vil.nai.com for the latest virus protection patches.

Viruses are usually spread through emails, so practice safe emailing (see below). Viruses are single programs designed to replicate and may or may not be malignant. Trojans are programs designed to give a third party (or anyone!) access to your computer.

An email address can be faked or used by someone other than the true owner. This can be done by obtaining access to another person's computer and password, by hacking into the service provider, or by using an address that appears to be the specific person's address. For example, by exchanging the lowercase "l" with the number "1", you can create a similar address and most people will not notice the difference.

To avoid being fooled by a spoof, use meaningful subject lines and periodically ask questions that only the true person could answer;

- 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. In Internet Explorer, go to Tools, then Options. In Netscape Navigator, go to Edit, then Preferences. While you're in either of these menus, delete all your history, any cookies you may have and empty your cache. Remember to delete all your bookmarks as well. Browsers also keep records of the site you visit in cache files, so find out which files should be deleted on your system.
- Upgrade all web browsers to support 128-bit encryption. This will help safeguard any information you want to pass securely over the web, including passwords and other sensitive data submitted on forms. Install the most recent security patches for all software used, especially Microsoft Office, Microsoft Internet Explorer and Netscape.
- Don't use a computer with delicate information stored on it for non-essential web browsing.

(e) Basic safe emailing

These are safe email practices which you and all your friends and associates should follow. Let them know that you will not open their email unless they practice safe emailing.

- NEVER open an email from someone you don't know.
- NEVER forward an email from someone you don't know, or which originated with someone you don't know. All those "think happy thoughts" emails that people send around could contain viruses. By sending them to your friends and associates you may be infecting their computers. If you like the sentiment enough, retype the message and send it out yourself. If retyping it is not worth your time, it's probably not that important a message.
- NEVER download or open an attachment unless you know what it contains and that it is secure. Turn off automatic download options in your email program. Many viruses and Trojans spread themselves as "worms" and modern worms often appear to have been sent by someone you know. Smart worms scan your address book, especially if you use Microsoft Outlook or Outlook Express, and replicate by masquerading as legitimate attachments from legitimate contacts. PGP signing your emails, both with and without attachments, can greatly reduce confusion over virus-free attachments you send to colleagues (PGP is a software to encrypt information, please see below under "Encryption")
- DON'T use HTML, MIME or rich text in your email - only plain text. Enriched emails can contain embedded programs which could allow access or damage your computer files.

- If using Outlook or Outlook Express, turn off the preview screen option.
- Encrypt your email whenever possible. An unencrypted email is like a postcard that can be read by anyone who sees it or obtains access to it. An encrypted email is like a letter in an envelope inside a safe.
- Use meaningful subject lines so the reader knows that you intended to send the message. Tell all your friends and colleagues to always say something personal in the subject line so you know they truly sent the message. Otherwise someone might be spoofing them, or a Trojan might have sent out an infected program to their entire mailing list, including you. However, don't use subject lines that give away secure information in encrypted emails. Remember, the subject line is not encrypted and can give away the nature of the encrypted mail, which can trigger attacks. Many hacking programs now automatically scan and copy email messages with "interesting" subjects such as "report", "confidential" "private" and other indications that the message is of interest.
- NEVER send email to a large group listed in the "To" or "CC" lines. Instead, send the message to yourself and include everyone else's name in the "bcc" lines. This is common courtesy as well as good privacy practice.
- NEVER respond to spam, even to request to be taken off the list. Spam servers send email to vast hoards of addresses and they never know which ones are "live" – meaning that someone is using the email address actively. By responding, the server recognizes you as a "live" account and you are likely to receive even more spam as a result.
- If possible, keep a separate computer, not connected to any other, that accepts general emails and contains no data files.

(f) General tips for internet cafes and beyond

Emails sent in plain text or unencrypted across the internet can be read by many different parties, if they make the effort to do so. One of these may be your local Internet Service Provider (ISP) or any ISP through which your emails pass. An email travels through many computers to get from the sender to the recipient; it ignores geopolitical boundaries and may pass through another country's servers even if you are sending emails within the same country.

Some general tips on issues commonly misunderstood by internet users:

- Password-protecting a file does so little to protect the file that it is not worth doing for documents containing sensitive information. It only provides a false sense of security.
- Zipping a file does not protect it from anyone wanting to see what is inside.
- If you want to make sure a file or email is sent securely, use encryption (see www.privaterra.com).
- If you want to send an email or a document securely, use encryption all the way to the final recipient. It is not good enough to send an encrypted email from a field office to New York or London or anywhere else and then have that same email forwarded unencrypted to another person.
- The internet is global in nature. There is no difference between sending an email between two offices in Manhattan and sending an email from an internet café in South Africa to a London office computer.

- Use encryption as often as possible, even if the email or data you are sending are not sensitive!
- Make sure the computer you are using has virus protection software. Many viruses are written to extract information from your computer, whether it be your hard drive contents or you email files, including email address books.
- Make sure your software is properly licensed. If you are using unlicensed software, you instantly become a software pirate instead of a human rights activist in the eyes of governments and media. The best option is to use open source software – it's free!
- There is no 100% secure solution if you are using the internet. Be aware that a person can "socially hack" into a system by pretending to be someone they are not on the phone or by email. Use your own judgement and common sense.

(g) Other important points:

- Always save encrypted email in encrypted form. You can always decrypt it again later, but if someone gains access to your computer, it is just as vulnerable as if it had never been encrypted.
- Be persistent with everyone with whom you exchange encrypted emails to make sure they do not decrypt and forward emails, or reply without bothering to encrypt them. Individual laziness is the biggest threat to your communications.
- You might wish to create a few safe email accounts for people in the field that are not generally used and so do not get picked up by spam servers. These addresses should be checked consistently but not used, except by field staff. This way you can destroy email addresses that are getting a lot of spam without endangering your contact base.

(h) Internet and the law

With the enactment of the Cyber Crimes Act, 2015, the Online Content Regulations, 2018, the Media Services Act, 2016, communication has become highly restricted. It is therefore important for a human rights defender to ensure;

- You never disseminate and/or forward messages on any social media that you are not sure of its authenticity. Cyber Crimes Act, 2015 is always there to catch you once you violate it.
- Keep your communications secure. You can download a free app known as Automatic Call recorder to keep all your communications and assist you in future references.
- Avoid disseminating ponographic or any other sexual photos or videos
- Avoid using insult language on any social media
- You do not run any online platform that is supposed to be registered but you have not registered the same.

NOTE: *The above is not an exhaustive list of what one should not do, HRDs are therefore encouraged to take their time to go through the aforementioned laws for ease of their references and understanding.*

Chapter

10 Assesing Organisational Security Performance

10.0 Introduction

As an organisation, it's likely that you already have some security measures in place. At the same time you probably feel if there is room for improvement – there usually is! Knowing where to start may seem overwhelming so it's a good idea to carry out an assessment to get a realistic overview of your existing organisational security first.

There are key people who should be included in this process. These may differ from organisation to organisation and it might be helpful to include external advisers to help guide the process too. For example:

Internal - Board of directors, executive director, management and senior staff, regular staff and volunteers.

External - Donors, external consultants and trainers

Involving each of these actors has advantages and disadvantages and it is important that the process is carried out in an inclusive, participative, transparent and non-judgemental manner. Formal hierarchies within organisations need to remain sensitive to the needs of their programme and 'field' staff or volunteers who may face greater risk in their day to day work. Staff and volunteers should also respect the fact that management face a difficult task in standardising an approach to security.

10.1 Criteria for assessment

We can begin by looking at some concrete issues and indicators to help assess how security protocols are observed by staff. Consider the following points:

- Acquired security experience: Do staff have experience of implementing security practices? Is this experience spread evenly across staff, or concentrated among a few individuals?
- Security training. Security training through courses or through individuals' own initiative during daily work. Resources, time and space need to be made available for training (either formal or informal). Is such training available to members of the organisation? Does this include training on psycho-social well-being and digital security?

- Attitudes and awareness: Are people aware of the importance of security and protection? Are their attitudes towards it positive and open to making improvements? What barriers do they perceive? Are attitudes and awareness regarding digital security, physical security and psycho-social well-being shared across the organisation?
- Security planning: To what extent is security planning integrated into our work? How often are context analyses carried out and security plans created? Are plans updated regularly, and do they include digital device management and stress management?
- Assignment of responsibilities: Is there a clear division of responsibilities for implementation of our security practices? To what extent are these responsibilities observed, and what are the potential blockages?
- Ownership and compliance of rules: How are people involved in the organisational security planning, and to what extent do they observe the plans that exist? What are the problems which arise here, and how can they be overcome? How can the process be made more participative?
- Response to security incidents: How often are security incidents shared? How often are they analysed and subsequently acted upon if necessary?
- Regular evaluation: How often are security strategies and plans updated? Is there a concrete process in place for this, or is it ad-hoc? How can it be made more regular? What other problems exist and how can they be overcome?

10.2 The Security Wheel

The above organisational self-assessment using the same criteria can objectively be conducted by implementing the security wheel and its eight spokes. The idea is that a wheel must be round to turn; in other words, all the spokes need to be of the same length. The same applies to the security wheel and its 8 spokes (components) representing the security management in an organisation or group of defenders.

This assessment can be done in groups of all actors in an organization as follows:

i. Sketch out the wheel

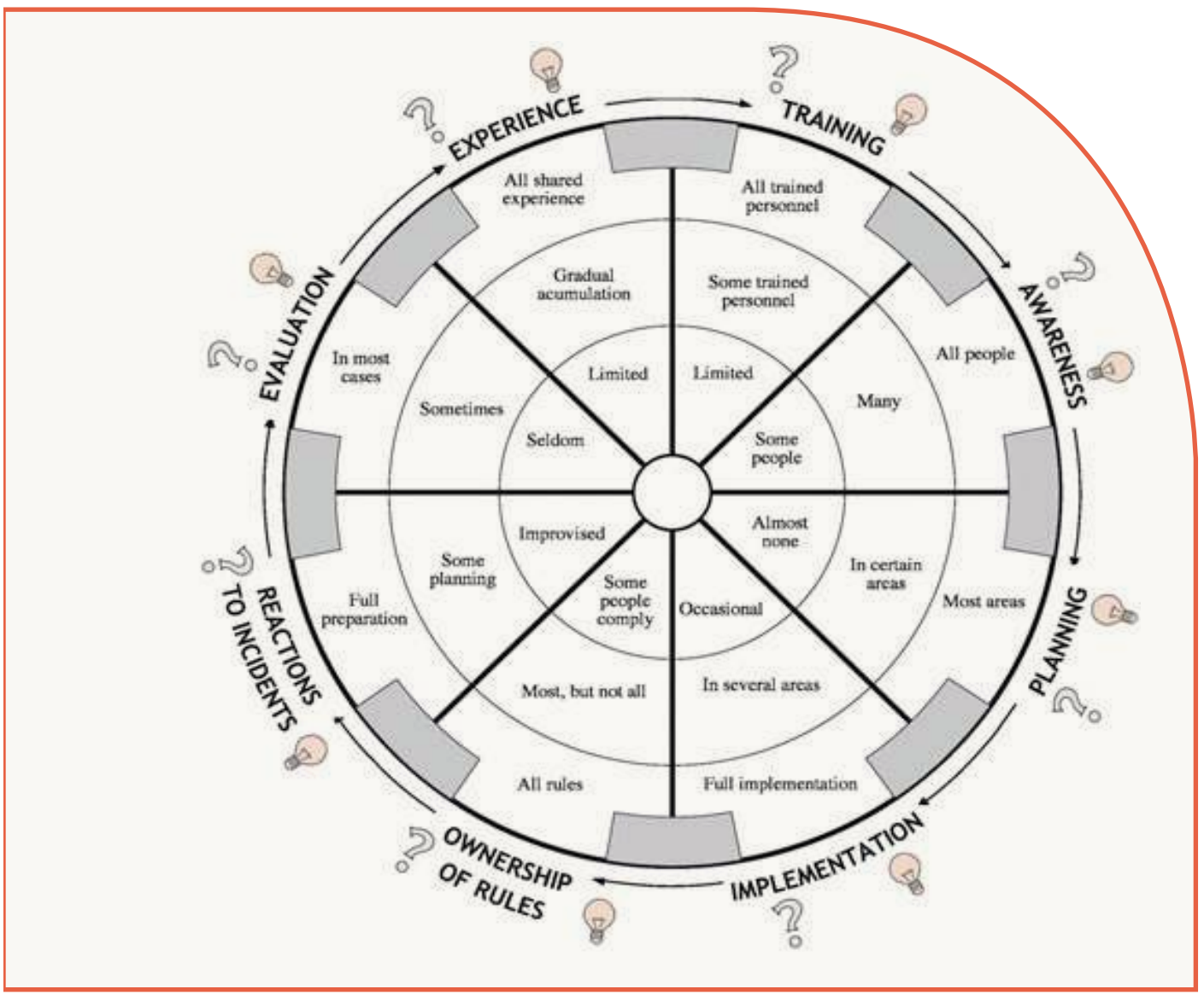
ii. Fill in each spoke according to how developed you think it is

iii. List reasons (brainstorming)why specific spokes are less developed; as all spokes must be at least as long as the most developed spoke, suggest ways of achieving that result: set objectives and relevant processes, anticipate possible problems and suggests solutions.

iv. Once you have completed this exercise, keep your security wheel and repeat the exercise a few months later. You will be able to compare both wheels and determine point by point whether things have improved.

A sample security wheel

The security wheel is never perfect: Some components are more developed than others. It is therefore more useful to determine the degree of development of each component. In this way, you can identify which types of action need prioritising in order to improve your protection and security. The dotted lines going from the centre to the outside edge illustrate how developed this component of the wheel is.



Draw the wheel onto the flap chart add colour to the gaps between the spokes to illustrate visually the actual shape of the wheel for your group or organization. You will then easily be able to see which components are more - and less - developed.

Chapter

11

Developing Security Plans and Implementing it

11.0 Introduction

A security plan is a document that includes preventive and reactive protection measures that improve personal or organizational safety and security. It is the roadmap for safety and security of the organization activities, staff, and primary stakeholders.

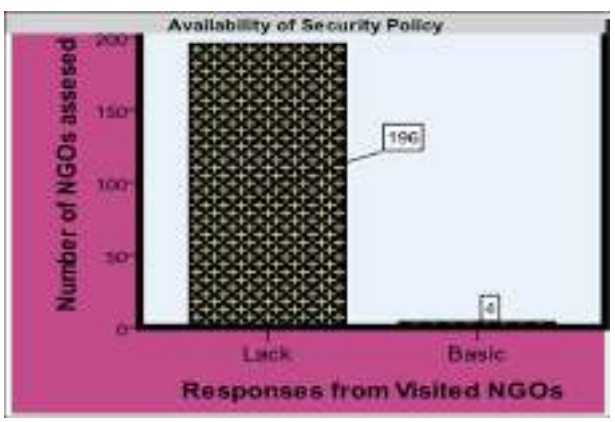
11.1 Differences between a Security Policy and Security Plan

A security policy is a set of general rules, principles, and guidelines within an organization to meet the needs of proper security management. A security plan can also focuses on the implementation of those rules, principles, and guidelines to fit a specific situation during a given period or activity undertaken by the organization.

For instance, an organisation may design a security plan while prepare to go to the field survey and sets general Rules or policies aimed at addressing the issue of staff travel.

11.2 HRDs and Security Plans in Tanzania

According to the THRDC's 2013 security needs assessment report, only four HRDNGOs out of the 200 visited had security policies with well-defined plans, rules and responsibilities. These four organizations were Action Aid Zanzibar, Care International Mwanza, OXFAM –Arusha and DONET in Dodoma.



Figures on the table above indicate that 196 HRNGOs assessed had no security policy or any other plan for their safety

As of the time this protection is written, more than 10 HRDNGOs have the security policies and plans in place. Some of these organizations are the Tanzania Women Lawyers Association, Tanzania Genders Networking Program (TGNP), Under the Same Sun (UTSS),the Coalition to Address Maternal Morbidity and Mortality due to Abortion and its Complications (CAMMAC) and the Legal and Human Rights centre(LHRC) to mention a few.

11.3 How to Develop a Security Plan

To come up with a security plan, staff members should meet to brainstorm about the organisation's potential risks. If you have done a risk assessment for your organisation, you might have a long list of vulnerabilities, several kinds of threats and a number of capacities. You can't realistically cover everything at the same time. So where to begin? It's very easy:

i. Select a few threats.

   Priorities the threats you have listed, be it actual or potential ones, using one of these criteria: The most serious threat -clear death threats, for example; OR the most probable and serious threat - if organizations similar to yours have been attacked, that is a clear potential threat for you; OR the threat which corresponds most with your vulnerabilities - because you are more at risk of that specific threat.

ii. List the vulnerabilities you have which correspond with the threats you have listed.

   These vulnerabilities should be addressed first, but remember that not all vulnerabilities correspond with all threats. For example; if you receive a death threat, it may not be very useful to start securing the cupboards in your office in the city centre (unless you can be easily attacked in the office, which is usually not the case). It may be more useful to reduce your exposure while commuting from home to the office or on weekends. Securing the cupboards isn't unimportant, but that in itself probably won't reduce your vulnerability to the death threat.

iii. List the capacities you have which correspond with the threats you have listed. You are now in a position to address the selected threats, vulnerabilities and capacities in your security plan, and can be reasonably sure that you will be able to reduce your risk from the right starting point.

Please note that this is an ad hoc way of drafting a security plan. There are more "formal" ways to do it, but this method is straightforward and makes sure you take care of the most urgent security issues - provided your risk assessment is correct - and end up with an "alive" and "real" plan at the end, and that's the important part of security.

11.4 Implementation of the Security Plan

Security plans are important, but they are not easy to implement. Implementation is much more than a technical process - it is an organizational process. It needs the involvement of all the staff and the support of the organization's management; Clear communication among all parties involved in its development as per the content; Measures to ensure adherence; Regular updates and reviews.

This means looking for entry points and opportunities, as well barriers and problems.

57A security plan must be implemented on at least three levels:

- The individual level.
  Each individual has to follow the plan in order for it to work.
- The organizational level.
  The organisation as a whole has to follow the plan.
- The inter-organizational level.
  Some level of cooperation between organizations is usually involved to maintain security.

Examples of entry points and opportunities when implementing a security plan:

- Several minor security incidents have taken place in your own or another organization and some staff members are worried about it.
- General security concerns exist because of the situation in the country.
- New staff arrives and can be trained to start good security practices more easily.
- Another organization offers you security training.

Examples of problems and barriers to implementing a security plan:

- Some people think more security measures will lead to an even greater workload.
- Others think the organization already has good enough security.
- Very busy for considering the plan
- It's not for the organization but for the people intend to be helped.

Chapter

12 Security and Free Time (Stress Management)

12.0 Introduction

While in some workplace stress is normal, excessive stress can interfere with your productivity and performance, impact your physical and emotional health, and affect your relationships and home life. It can even mean the difference between success and failure on the job. You can't control everything in your work environment, but that doesn't mean you're powerless—even when you're stuck in a difficult situation. Whatever your ambitions or work demands, there are steps you can take to protect yourself from the damaging effects of stress, improve your job satisfaction, and bolster your well-being in and out of the workplace. Human Rights Defenders like any other group of people are faced with stress because of their work. These guidelines are therefore a guide to reducing and/or preventing stress under this part;

12.1 When is workplace stress too much?

Stress isn't always bad. A little bit of stress can help you stay focused, energetic, and able to meet new challenges in the workplace. It's what keeps you on your toes during a presentation or alert to prevent accidents or costly mistakes. But in today's hectic world, the workplace too often seems like an emotional roller coaster. Long hours, tight deadlines, and ever-increasing demands can leave you feeling worried, drained, and overwhelmed. And when stress exceeds your ability to cope, it stops being helpful and starts causing damage to your mind and body—as well as to your job satisfaction.

If stress on the job is interfering with your work performance, health, or personal life, it's time to take action. No matter what you do for a living, or how stressful your job is, there are plenty of things you can do to reduce your overall stress levels and regain a sense of control at work.

12.2 Tips to dealing with Stress

(a) Beat workplace stress by reaching out

Sometimes the best stress-reducer is simply sharing your stress with someone close to you. The act of talking it out and getting support and sympathy—especially face-to-face—can be a highly-effective way of blowing off steam and regaining your sense of calm. The other person doesn't have to "fix" your problems; they just need to be a good listener.

(b) Turn to co-workers for support. Having a solid support system at work can help buffer you from the negative effects of job stress. Just remember to listen to them and offer support when they are in need as well. If you don't have a close friend at work, you can take steps to be more social with your co-workers. When you take a break, for example, instead of directing your attention to your smartphone, try engaging your colleagues.

(c) Lean on your friends and family members. As well as increasing social contact at work, having a strong network of supportive friends and family members is extremely important to managing stress in all areas of your life. On the flip side, the lonelier and more isolated you are, the greater your vulnerability to stress.

(d) Build new satisfying friendships. If you don't feel that you have anyone to turn to—at work or in your free time—it's never too late to build new friendships. Meet new people with common interests by taking a class or joining a club, or by volunteering your time. As well as being a great way to expand your social network, being helpful to others—especially those who are appreciative—delivers immense pleasure and can help to significantly reduce stress.

(e) Support your health with exercise and nutrition

When you're overly focused on work, it's easy to neglect your physical health. But when you're supporting your health with good nutrition and exercise, you're stronger and more resilient to stress. Taking care of yourself doesn't require a total lifestyle overhaul. Even small things can lift your mood, increase your energy, and make you feel like you're back in the driver's seat.

(f) Make time for regular exercise

Aerobic exercise—activity that raises your heart rate and makes you sweat—is a hugely effective way to lift your mood, increase energy, sharpen focus, and relax both the mind and body. Rhythmic movement—such as walking, running, dancing, drumming, etc.—is especially soothing for the nervous system. For maximum stress relief, try to get at least 30 minutes of activity on most days. If it's easier to fit into your schedule, break up the activity into two or three shorter segments.

And when stress is mounting at work, try to take a quick break and move away from the stressful situation. Take a stroll outside the workplace if possible. Physical movement can help you regain your balance.

Your food choices can have a huge impact on how you feel during the work day. Eating small, frequent and healthy meals, for example, can help your body maintain an even level of blood sugar, keeping your energy and focus up, and avoiding mood swings. Low blood sugar, on the other hand, can make you feel anxious and irritable, while eating too much can make you lethargic.

(g) Eat healthy.

- Minimize sugar and refined carbs. When you're stressed, you may crave sugary snacks, baked goods, or comfort foods such as pasta or French fries. But these "feel-good" foods quickly lead to a crash in mood and energy, making symptoms of stress worse not better.

- Reduce your intake of foods that can adversely affect your mood, such as caffeine, trans fats, and foods with high levels of chemical preservatives or hormones.
- Avoid nicotine. Smoking when you're feeling stressed may seem calming, but nicotine is a powerful stimulant, leading to higher, not lower, levels of anxiety.
- Drink alcohol in moderation. Alcohol may seem like it's temporarily reducing your worries, but too much can cause anxiety as it wears off and adversely affect your mood.

(h) Don't skip sleeping

You may feel like you just don't have the time get a full night's sleep. But skimping on sleep interferes with your daytime productivity, creativity, problem-solving skills, and ability to focus. The better rested you are, the better equipped you'll be to tackle your job responsibilities and cope with workplace stress.

- Improve the quality of your sleep by making healthy changes to your daytime and nightly routines. For example, go to bed and get up at the same time every day, even on weekends, be smart about what you eat and drink during the day, and make adjustments to your sleep environment. Aim for 8 hours a night—the amount of sleep most adults need to operate at their best.
- Turn off screens one hour before bedtime. The light emitted from TV, tablets, smartphones, and computers suppresses your body's production of melatonin and can severely disrupt your sleep.
- Avoid stimulating activity and stressful situations before bedtime such as catching up on work. Instead, focus on quiet, soothing activities, such as reading or listening to soft music, while keeping lights low.

(i) Prioritize and organize

When job and workplace stress threatens to overwhelm you, there are simple, practical steps you can take to regain control.

- Create a balanced schedule. All work and no play is a recipe for burnout. Try to find a balance between work and family life, social activities and solitary pursuits, daily responsibilities and downtime.
- Leave earlier in the morning. Even 10-15 minutes can make the difference between frantically rushing and having time to ease into your day. If you're always running late, set your clocks and watches fast to give yourself extra time and decrease your stress levels.
- Plan regular breaks. Make sure to take short breaks throughout the day to take a walk, chat to a friendly face, or practice a relaxation technique. Also try to get away from your desk or work station for lunch. It will help you relax and recharge and be more, not less, productive.
- Establish healthy boundaries. Many of us feel pressured to be available 24 hours a day or obliged to keep checking our smartphones for work-related messages and updates. But it's important to maintain periods where you're not working or thinking about work. That may mean not checking emails or taking work calls at home in the evening or at weekends.

- Don't over-commit yourself. Avoid scheduling things back-to-back or trying to fit too much into one day. If you've got too much on your plate, distinguish between the "shoulds" and the "musts." Drop tasks that aren't truly necessary to the bottom of the list or eliminate them entirely.

(j) Task management tips for reducing job stress

- Prioritize tasks. Tackle high-priority tasks first. If you have something particularly unpleasant to do, get it over with early. The rest of your day will be more pleasant as a result.
- Break projects into small steps. If a large project seems overwhelming, focus on one manageable step at a time, rather than taking on everything at once.
- Delegate responsibility. You don't have to do it all yourself. Let go of the desire to control every little step. You'll be letting go of unnecessary stress in the process.
- Be willing to compromise. Sometimes, if you can both bend a little at work, you'll be able to find a happy middle ground that reduces the stress levels for everyone.

(k) Break bad habits that contribute to workplace stress

Many of us make job stress worse with negative thoughts and behavior. If you can turn around these self-defeating habits, you'll find employer-imposed stress easier to handle.

- Resist perfectionism. When you set unrealistic goals for yourself, you're setting yourself up to fall short. Aim to do your best, no one can ask for more than that.
- Flip your negative thinking. If you focus on the downside of every situation and interaction, you'll find yourself drained of energy and motivation. Try to think positively about your work, avoid negative-thinking co-workers, and pat yourself on the back about small accomplishments, even if no one else does.
- Don't try to control the uncontrollable. Many things at work are beyond our control—particularly the behavior of other people. Rather than stressing out over them, focus on the things you can control such as the way you choose to react to problems.
- Look for humor in the situation. When used appropriately, humor is a great way to relieve stress in the workplace. When you or those around you start taking things too seriously, find a way to lighten the mood by sharing a joke or funny story.
- Clean up your act. If your desk or work space is a mess, file and throw away the clutter; just knowing where everything is can save time and cut stress.
- Be proactive about your job and your workplace duties. When we feel uncertain, helpless, or out of control, our stress levels are the highest. Here are some things you can do to regain a sense of control over your job and career.
- Talk to your employer about workplace stressors. Healthy and happy employees are more productive, so your employer has an incentive to tackle workplace stress whenever possible. Rather than rattle off a list of complaints, let your employer know about specific conditions that are impacting your work performance.

- Clarify your job description. Ask your supervisor for an updated description of your job duties and responsibilities. You may then be able to point out that some of the things you are expected to do are not part of your job description and gain a little leverage by showing that you've been putting in work over and above the parameters of your job.
- Request a transfer. If your workplace is large enough, you might be able to escape a toxic environment by transferring to another department.
- Ask for new duties. If you've been doing the exact same work for a long time, ask to try something new: a different grade level, a different sales territory, a different machine.
- Take time off. If burnout seems inevitable, take a complete break from work. Go on vacation, use up your sick days, ask for a temporary leave-of-absence—anything to remove yourself from the situation. Use the time away to recharge your batteries and take perspective.

(l) How Bosses Reduce Work Stress

- Consult your employees. Talk to them about the specific factors that make their jobs stressful. Some things, such as failing equipment, understaffing, or a lack of supervisor feedback may be relatively straightforward to address. Sharing information with employees can also reduce uncertainty about their jobs and futures.
- Communicate with your employees one-on-one. Listening attentively face-to-face will make an employee feel heard and understood—and help to lower their stress and yours—even if you're unable to change the situation.
- Deal with workplace conflicts in a positive way. Respect the dignity of each employee; establish a zero-tolerance policy for harassment.
- Give workers opportunities to participate in decisions that affect their jobs. Get employee input on work rules, for example. If they're involved in the process, they'll be more committed.
- Avoid unrealistic deadlines. Make sure the workload is suitable to your employees' abilities and resources.
- Clarify your expectations. Clearly define employees' roles, responsibilities, and goals. Make management actions fair and consistent with organizational values.
- Offer rewards and incentives. Praise good work performance verbally and organization-wide. Schedule potentially stressful periods followed by periods of fewer tight deadlines. Provide opportunities for social interaction among employees.

References and useful Links

1. Protection Manual for Human Rights Defenders; 2005; By FrontLine Defenders
2. The Situation Reports of HRDs in Tanzania, 2013, 2014, 2015, 2016 and 2017; By Tanzania Human Rights Defenders Coalition
3. Security Guide for Human Rights Defenders in Africa; 2017; By Defend Defenders

Useful Links

http://locdoc.net/security-and-locksmithing-blog/8-simple-steps-you-can-take-to-improve-your-office-security-today/

https://www.helpguide.org/articles/stress/stress-in-the-workplace.htm

https://www.apa.org/helpcenter/work-stress.aspx

https://security.berkeley.edu/resources/best-practices-how-to-articles/top-10-secure-computing-tips

https://www.zdnet.com/article/simple-security-step-by-step-guide/

https://www.theguardian.com/technology/2013/sep/16/10-ways-keep-personal-data-safe

https://www.afgonline.com.au/learn/home/top-10-tips-to-improve-your-home-security/

List of Statutes

1. Cyber Crimes Act, 2015
2. Media Services Act, 2016
3. Access to Information Act, 2017
4. Online Content Regulations, 2018
5. Police Force and Auxiliary Services Act, 1969
6. Regional Administration Act, 1997

Mwongozo wa usalama na Ulinzi kwa Watetezi wa Haki za Binadamu Tanzania

MTANDAO WA WATETEZI WA HAKI ZA BINADAMU TANZANIA

Mwongozo wa usalama na Ulinzi kwa Watetezi wa Haki za Binadamu Tanzania

Umeandaliwa na:
Wakili Jones Sendodo
Wakili Deogratias Bwire

Umehaririwa na
Onesmo Olengurumwa

Yaliyomo

Utangulizi

Mtandao wa Watetezi wa Haki za Binadamu Tanzania (THRDC) ni shirika lisilo la kiserikali, lililosajiliwa chini ya Sheria ya mashirika yasiyo ya Serikali ya mwaka 2002. THRDC inajumuisha wanachama binafsi na washirika ambao hadi mwaka 2018 wanakadiriwa kuwa 150 nchini kote Tanzania. Uanachama wake na uwakilishi umeenea katika suala la (kwa njia ya makundi mbalimbali ya utetezi wa haki za binadamu na uwakilishi wa takribani kanda 11) katika Jamhuri ya Muungano wa Tanzania (bara na visiwani).

Madhumuni makuu ya mtandao huu ni pamoja na kazi ya kutetea na kuhamasisha usalama na ulinzi kwa Watetezi wa Haki za Binadamu Tanzania. Katika kukamilisha hili, Mtandao umejikita katika kuboresha usalama kwa watetezi nchini na pia kutoa utetezi wa moja kwa moja. Pia mtandao umejipanga kuimarisha matumizi ya mbinu za kikanda na kimataifa kwa watetezi nchini ili kulinda na kukuza uelewa wa haki na majukumu ya watetezi wa haki za binadamu.

Matokeo ya mwisho ya mtandandao huu yanatarajiwa kuonyesha mchango wa katika kuimarisha mazingira salama ya kazi kwa watetezi wa haki za binadamu nchini. Mtandao umekuwa na bado unatarajia kufanya kazi kwa karibu na wadau mbalimbali ikiwa ni pamoja na mashirika ya ndani nchi, kikanda na ya kimataifa ya watetezi wa haki za binadamu, Watetezi binafsi; wadau wa maendeleo; Taasisi za Umoja wa Mataifa; mamlaka za umma na wadau wengine.

Mwongozo huu wa usalama na ulinzi umejaribu kurahisisha taarifa mbalimbali ambazo watetezi wa haki za binadamu wanapaswa kuelewa kwa ajili ya usalama wao. Taarifa zilizo katika muongozo huu zilikusanywa kutoka maeneo mbalimbali ambayo marejeo yanayotolewa katika ukurasa wa mwisho.

Dibaji

Mwongozo huu unatoa maelezo juu ya hatua mbalimbali za usalama kujikinga ambazo mtetezi wa haki za binadamu anaweza kuchukua ili kupunguza na / au kuzuia hatari zinazowakabiri. Muongozo huu unajumuisha sura 12 tofauti. Sura zinahusisha masuala kama usalama wa kidijitali, mwitikio juu ya matukio ya usalama, tathmini ya hatari na usimamizi, mpango wa usalama, , usalama nyumbani na ofisini, usalama wa mtetezi akiwa chini ya ulinzi. Hizi pamoja na hatua zingine zinatarajiwa kuwasaidia watetezi wa haki za binadamu wanapokabiliwa na hatari kabla ya kutafuta msaada mkubwa kutoka kwa mashirika ya ulinzi na utetezi wa haki za binadamu au vyombo vya kutekeleza sheria.

Sura ya

1

Uchambuzi wa Hali na Kimuktadha

1.0 Utangulizi

Kupitishwa kwa Azimio la Umoja wa Mataifa juu ya Watetezi wa Haki za Binadamu mwaka 1998 na kuanzishwa kwa mamlaka ya Msimamizi maalum wa Umoja wa Mataifa juu ya hali ya watetezi wa haki za binadamu mwaka 2000 ni muhimu sana katika ulinzi wa watetezi wa haki za binadamu duniani kote. Hata hivyo, watetezi wa haki za binadamu wanaendelea kukabiliwa na vitisho na hatari licha ya kuwepo kwa taratibu hizi.

Barani Afrika, watetezi wa haki za binadamu wanaofanya kazi ya kuhamasisha na kulinda haki za binadamu katika mazingira ya sasa ya kisiasa hukabiliwa na hatari kubwa, kama vile mauaji, mashambulizi, kukamatwa, mashtaka ya kughushi , utekaji nyara, kutokujali kwa serikali kuhusu usalama wa watetezi, kutishiwa na kuminywa kwa nafasi kiraia. Nchi nyingi zimekuwa hazisimamii uchunguzi wa ukiukwaji wa haki za watetezi. Ili kuhakikisha usalama na kuendelea kwa kazi zao, watetezi wamechukua hatua za kusimamia usalama wao binafsi na mashirika yao kwa kutathmini hatari na kuweka mikakati yenye ufanisi ili kupunguza vitisho vingi.

Kutoa muda na rasilimali kusimamia usalama husaidia watetezi wa haki za binadamu (HRDs) kuendelea na shughuli za haki za binadamu na kuhakikisha usalama na ulinzi wao. Mtandao wa Watetezi wa Haki za Binadamu Tanzania (THRDC) umeweka katika muktadha muongozo wa usalama kwa watetezi wa haki za binadamu inayolenga kutumika kama zana kwa watetezi wa haki za binadamu nchini Tanzania ili kuwapa mikakati na majibu muhimu kwa mazingira ya kawaida ambamo yanafanyia kazi.

1.1 Hali ya sasa

THRDC imekuwa ikianda na kuchapisha Ripoti za Hali za Mwaka za watetezi wa haki za binadamu nchini Tanzania tangu mwaka 2013-2017. Ripoti hizi zinaonyesha kuwa, hali ya watetezi wa haki za binadamu nchini huwa mbaya zaidi kadri muda unavyokwenda. Matukio yanayojulikana zaidi ambayo yanaonyesha mazingira mabaya ambamo watetezi wa haki za binadamu wanafanyia kazi ni pamoja na, kuminywa kwa nafasi ya kiraia, kukamatwa kiholela, mashtaka ya kughusi, watetezi kupewa majina ya kihalifu na sifa mbaya, kupotea kwa uhuru wa kujieleza na haki ya kupata

taarifa, vitisho,mashambulizi na kadhalika.. Ripoti hizi zinasaidia kuujulisha umma na jumuia za kimataifa juu ya kupanga njia bora za kukabiliana na matatizo yanayowakabili watetezi wa haki za binadamu (HRDs) na kuhakikisha mazingira yao ya kazi daima ni salama. Kwa madhumuni ya Muongozo huu wa hali ya uchambuzi itaonekana katika maeneo yafuatayo;

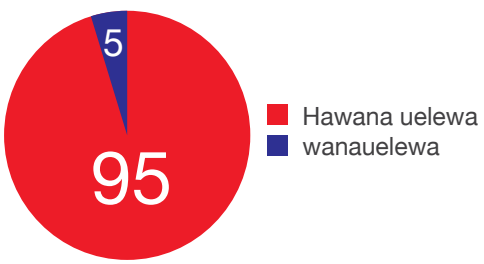
1.2 Ni nani watetezi wa Haki za Binadamu?

Watetezi wa haki za binadamu ni watu ambao, kwa kibinafsi au pamoja na wengine, wanafanya kazi za kuhamasisha au kulinda haki za binadamu zilizotajwa katika Azimio la Umoja wa Mataifa la Haki za Binadamu 1948 (UDHR). Azimio la Umoja wa Mataifa la Watetezi wa Haki za Binadamu la 1998 linawaelezea watetezi kama; “watu binafsi, makundi na vyama vinavyochangia kuondokana na ukiukaji wa haki zote za binadamu na uhuru wa msingi wa watu na watu binafsi.” Mtu yeyote anaweza kuwa mtetezi wa haki za binadamu bila kujali historia ya elimu, sifa za kitaaluma, jinsia, umri, rangi, kundi la kijamii, au taifa. Ikiwa ni machinga au muuzaji wa ndizi anakemea unyanyasaji wa wauzaji wenzake kutoka kwa na mamlaka za mitaa za kodi z, huyu anaonekana kuwa mtetezi wa haki za binadamu . Katika hali nyingine, watetezi wanaweza kupatikana katika sekta binafsi na za serikali. Hata hivyo, ni muhimu kusisistiza kuwa hatua zote zilizochukuliwa na mtetezi katika utetezi wa haki za binadamu lazima ziwe za amani.

1.3 Kiwango cha Uelewa wa njia mbalimbali za Usimamizi wa Usalama kwa Watetezi

Kwa mujibu wa ripoti ya tathmini ya mahitaji ya watetezi ya 2013, dhana ya mtetezi wa haki za binadamu (HRD) ilikuwa haijulikani sana katika muktadha wa Tanzania. Majukumu na haki za mtetezi wa haki za binadamu havikujulikana sana hata kwa watetezi waliokuwepo. Aidha, watetezi hawakujua chochote kuhusu utaratibu wa usalama na ulinzi kwa ajili yao ikiwa ni katika ngazi za ndani ya nchi, za kikanda au za kimataifa Ripoti hiyo ilitoa taarifa zaidi kuwa watetezi wa haki za binadamu wengi hawajui mbinu za usalama wa kawaida na zile za teknolojia ya kidijitali.

Takribani asilimia 95 ya mashirika yasiyokuwa ya haki za binadamu yaliyotembelewa wakati wa uchunguzi hawana uelewa juu ya hatua na njia za usalama kwa watetezi.



Chati duara iliyochorwa hapo juu inaonesha asilimia ya ufahamu (kutoka kwa jumla ya watetezi 200 waliotembelewa) katika taarifa ya tathmini ya mahitaji ya watetezi wa haki za binadamu nchi kabla ya mwaka 2013. Sehemu yenye rangi nyekundu inawakilisha watetezi ambao hawakujua (95%) na sehemu ya bluu (5) %) ni kwa wale watetezi wenye ufahamu au wanaojua utaratibu wa usalama na ulinzi.

1.4 Vitendo vya Ukiukaji wa Haki za Binadamu dhidi ya Watetezi

Hali ya watetezi wa haki za binadamu (katika kipindi cha miaka mitano ya kuwepo kwa THRDC inaonyesha kuwa watetezi wa haki za binadamu wanaofanya kazi za utetezi wa haki za jamii za wafugaji, , waandishi wa habari, na haki za kiraia na kisiasa wamekuwa waathirika wa ukiukwaji. Chanzo cha ukiukwaji hutokana na kutokuwepo kwa hali ya serikali kutokuchukua hatua mara kwa mara dhidi ya vitendo vya ukiukwaji wa haki za watetezi, kuwepo kwa sheria kandamizi zile mpya na zilizotungwa kitamboz, hali ya kisiasa, na utawala uliopo serikalinikutokuheshimu Utawala wa Sheria. Pia, utekelezaji wa sheria kandamizi, kama vile Sheria ya Huduma za Vyombo vya Habari ya 2016, Sheria ya Makosa ya Mtandao ya 2015, Sheria ya Huduma za za Polisi, 1969, Sheria ya Wakuu wa Mikoa ya 1997 ambazo ni baadhi tu. Mtandao kwa kawaida hutoa huduma za msaada hususani matibabu, uwakilishi wa kisheria, na uhamisho wa muda mfupi ili kuwasaidia watetezi katika hatari. Jedwali hapo chini linaonyesha muhtasari wa matukio yaliyoandikwa ili kuonyesha hali hiyo kwa idadi

Mwaka	Idadi ya Matukio Yaliyorekodiwa
2013	Matukio 13
2014	Matukio 31
2015	Matukio 25
2016	Matukio 40
2017	Mtukio 46

Kati ya matukio yaliyorekodiwa hapo juu matukio mengi yanahusiana na mashtaka ya kughushi, kuminywa kwa uhuru, vitisho, mateso, kuminya uhuru wa kujieleza, kupiga marufuku magazeti, uvamizi wa nyumba za vyombo vya habari, mauaji, na mashambulizi miongoni mwa mengine.

Sura ya

2

Kufanya Maamuzi Sahihi juu ya Usalama na Ulinzi

2.0 Utangulizi

Kuyatambua mazingira ya kazi ya watetezi wa haki za binadamu ni muhimu kwa utendaji bora wa watetezi wa haki za binadamu. Kwa hiyo ni muhimu kwa watetezi wa haki za binadamu (HRDs) kujifunza mbinu tofauti za kufanya uchambuzi wa muktadha wa wadau.

2.1 Mazingira ya Kazi ya Watetezi wa Haki za Binadamu

Watetezi wa haki za binadamu kawaida hufanya kazi katika mazingira magumu, ambapo kuna watendaji wengi tofauti, na ambao huathiriwa na mchakato wa maamuzi ya kisiasa. Mambo mengi hutokea kwa mtiririko jambo moja likiwa na athari kwa linguine. Mienendo ya kila mtendaji, au mdau, katika hali hii huchukua nafasi muhimu katika mahusiano ya mtendaji na watu wengine. Kwa hiyo watetezi wanahitaji taarifa sio tu juu ya masuala ya moja kwa moja kuhusiana na kazi zao, lakini pia kuhusu nafasi za watendaji muhimu na wadau. Watetezi wa haki za binadamu wanapaswa kuandaa kikundi cha kutathmini hali ili kujaribu kutambua na kuorodhesha watendaji wa kijamii, wa kisiasa na wa kiuchumi ambao wanaweza kuwa na ushawishi katika hali yako ya sasa ya usalama.

2.2 Kuchambua mazingira yako ya kazi

Ni muhimu kufahamu na kuelewa iwezekanavyo kuhusu mazingira unayofanyia kazi. Uchunguzi mzuri wa hali hiyo huwezesha maamuzi yenye taarifa juu ya sheria na taratibu za usalama zinazoweza kutumika. Pia ni muhimu kutafakari juu ya matukio ya uwezekano wa baadaye, ili, iwezekanavyo, kuchukua hatua ya kuzuia.

Hata hivyo, kuyachambua mazingira yako tu ya kazi haitoshi. Pia unahitaji kuangalia jinsi kila mwingiliano unaweza kuathiri hali na jinsi watendaji wengine wanaweza kuitikia kila mmoja. Pia ni muhimu kuzingatia vipimo vya mazingira ya kazi. Unaweza kufanya uchambuzi katika kiwango kikubwa kwa kujifunza na kuilewa nchi au kanda, lakini pia unahitaji kujua jinsi nguvu hizi zinafanya kazi katika eneo fulani ambako unafanya kazi, yaani, mienendo . Kwa mfano, mgambo wa eneo moja huenda wakatenda tofauti jinsi unavyoweza kutarajia kufuata uchambuzi wa kikanda au

kitaifa. Unahitaji kuwa na ufahamu wa sifa hizo za ndani. Pia ni muhimu ili kuepuka kuwa na mtazamo thabiti wa hali ya kazi, kwa sababu hali hukua na kubadilika. Kwa hiyo wanapaswa kupitiwa mara kwa mara. Kuuliza maswali, Uchambuzi wa nyanjani na Uchambuzi wa Wadau ni mbinu tatu muhimu za kuchambua mazingira yako ya kazi:

(a) Kuuliza maswali

Unaweza kuelewa mazingira yako ya kazi vizuri kwa kuuliza maswali sahihi kuhusu suala hilo. Njia hii ni chombo muhimu kwa kuzalisha majadiliano katika kundi dogo, lakini kitatumika tu ikiwa maswali yameandaliwa kwa namna ambayo itakuwa rahisi kupata suluhisho.

Kwa mfano, unyanyasaji wa viongozi wa serikali za mitaa umekuwa tatizo. Ikiwa unauliza swali kama: “Ni nini kinachopaswa kufanyika ili kupunguza unyanyasaji? Unaweza kuwa umepata dawa ya dalili za tatizo, yaani unyanyasaji.

Lakini ikiwa umeuliza swali lenye kuelezea suluhisho, unaweza kuwa kwenye njia yako ya kupata suluhisho halisi. Kwa mfano, ukiuliza: “Je! Mazingira yetu ya kijamii na kisiasa yana usalama kwa kufanyaji kazi yetu?”, hapa kuna majibu mawili tu - ndiyo au hapana.

Ikiwa jibu ni ndiyo, unahitaji kuunda swali lingine ambalo linaweza kukusaidia kuelezea na kuelewa vizuri masuala muhimu kwa ajili ya kuimarisha usalama wako. Ikiwa, baada ya kuzingatia vizuri shughuli zote zilizopo, mipango na rasilimali, pamoja na sheria, majadiliano, kulinganisha na watetezi wengine katika eneo hilo, nk, jibu linapaswa kuwa hapana, hili lenyewe itakuwa kiasi cha suluhisho cha tatizo la usalama.

(b) Namna ya Kutumia njia hii ya Kuuliza Maswali :

- Kuangalia maswali ambayo yatakazia hoja na kuelewa vizuri masuala muhimu yanayohusika kwa kuimarisha usalama wako.
- Kuunda maswali yenye kuleta ufumbuzi.
- Kurudia mchakato huu mara nyingi iwezekanavyo.

(c) Baadhi ya maswali muhimu ya kuulizwa:

- Je! Ni mambo gani muhimu yanayohusika zaidi katika tasnia ya kijamii, kisiasa na uchumi kwa wakati huu?
- Ni wadau wapi muhimu wanaohusika na mambo haya muhimu?
- Ni kwa jinsi gani kazi yetu inaweza kuwa naathari chanya au hasi katika maslahi ya wadau hawa muhimu?
- Je muitikio wetu unaweza kuwa vipi endapo tutakuwa tunawindwa yeyote kati ya watendaji hawa kutokana na kazi yetu?

- Je, Mazingira yetu ya kijamii na kisiasa yana usalama kwa kufanya kazi yetu?
- Je, mamlaka za ndani / kitaifa zimeitikia kwa namna gani kazi za awali za watetezi wa haki kuhusiana na suala hili?
- Je, Vyombo vya habari na jamii vimeitikia vipi katika mazingira sawa?.

(c) Uchambuzi wa nyanjani

Uchambuzi wa nyanjani ni mbinu ambayo inaweza kukusaidia kuibua jinsi vikundi tofauti vinavyosaidia au kuzuia ufanisi wa malengo yako ya kazi. Inaonyesha nguvu zote zinazosaidia na zinazopinga, na hufanyia kazi udhanifu kuwa matatizo ya usalama yanaweza kutokea kutokana na nguvu ya kupinga, na kwamba unaweza kuchukua faida ya nguvu tetezi ama saidizi. Mbinu hii inaweza kukamilishwa na mtu mmoja tu, lakini inafaa zaidi wakati unatumiwa na kikundi tofauti na lengo la kazi lililoeleweka na njia ya kulitimiza.

Anza kwa kuchora mshale wa ulalo unaoelekea kwenye sanduku. Andika muhtasari mfupi wa lengo lako la kazi katika sanduku hili. Hii itatoa lengo la kutambua nguvu saidizi na pinzani za kusaidia na kupinga. Chora sanduku jingine juu ya mshale wa kati. Weka nguvu zote ambazo zinaweza kukuzuia kufikia lengo lako la kazi hapa. Chora sanduku lililofanana, lenye nguvu zote za kusaidia, chini ya mshale. Chora sanduku la mwisho kwa ajili ya ambazo mwelekeo wake haijulikani au hauna uhakika.

Chati ya 1: uchambuzi wa nyanjani kwa kuchunguza mazingira ya ufanyaji kazi

Baada ya kukamilisha chati yako ni wakati mwafaka wa kutathmini matokeo. Uchambuzi wa nyanjani unasaidia kuona na kutafakari juu ya nguvu inayoshughulika nayo. Lengo ni kutafuta njia za kupunguza au kuondoa hatari zinazozalishwa na nguvu pinzani, kwa namna moja, kwa msaada kutoka kwa vikosi vya kusaidia. Kwa upande kupitia usaidizi muhimu kutoka njia saidizi. Katika nguvu zenye mwelekeo usiojulikana, utahitaji kuamua ama utawaweka kama wanaokuunga mkono, au utaendelea kuwafuatilia kwa karibu ili kuchunguza dalili zao kuwa ama wanakupinga au wanakuunga mkono.

(e) Uchambuzi wa wadau

Uchambuzi wa wadau ni njia muhimu ya kuongeza taarifa zinazopatikana wakati wa kufanya maamuzi juu ya ulinzi. Inahusisha kutambua na kuelezea watendaji tofauti au wadau wanaohusika na uhusiano wao, kwa misingi ya sifa zao na maslahi yao - yote kuhusiana na suala la ulinzi fulani.

Mshirika au mdau katika ulinzi ni mtu yeyote, kikundi au taasisi inayohusika na, au kuhusika kwenye matokeo ya sera katika eneo la ulinzi.

Uchambuzi wa wadau ni muhimu kwa kuelewa:

- yupi ni mdau na ni kwa hali gani udau wao unahusika Uhusiano kati ya wadau katika ulinzi, tabia zao na maslahi. Ni kwa jinsi gani hivi vitaathirika na shughuli za ulinzi.
- Kila nia ya mdau kushiriki katika shughuli hizo za ulinzi.

(f) Tunataka kupanua kazi yetu maeneo jirani

- Makampuni yenye nguvu yanayotumia rasilimali.
- Maafisa wa serikali ambao wanafaidika na rushwa.
- Kampuni moja imekubali kusimamisha unyonyaji
- Mashirika yasiyo ya kiserikali ya kimataifa yanasaidia kazi yetu.
- Tuna uzoefu wa kutosha na nafasi nzuri ya kijografia

Wadau katika ulinzi wanaweza kugawanywa kwa njia ifuatayo:

(i) Wahusika Wakuu

Katika mazingira ya ulinzi, hawa ni watetezi wenyewe, na wale wanaofanya kazi nao, kwa sababu wote wana sehemu ya msingi katika ulinzi wao wenyewe.

(ii) Wadau wenye wajibu, ambao ni wajibu wa kulinda watetezi, ambao ni:-

- Serikali na taasisi za dola (ikiwa ni pamoja na vikosi vya usalama, majaji, wabunge, nk)
- Vyombo vya kimataifa vyenye mamlaka inayojumuisha ulinzi, kama vyombo vya Uma oja wa Mataifa , Mashirikia ya Kikanda , , vikosi vya kulinda amani, nk.
- Kwa watendaji waliojihami wa silaha, wanaweza kuwajibika kwa kosa la kutoshambulia watetezi (kama raia), hasa wakati watendaji hawa wanadhibiti eneo hilo.

(g) Wadau muhimu, ambao wanaweza kuchochea ulinzi wa watetezi wa haki za binadamu.

Wanaweza kuwa na ushawishi wa kisiasa au uwezo wa kuweka shinikizo kwa wadau wenye wajibu wa ambao hawatimizi majukumu yao (kama vile serikali zingine, vyombo vya Umoja wa Mataifa, ICRC, nk), na vile vile baadhi yao yanaweza kuhusika katika mashambulizi na mashinikizo ya moja kwa moja au yasiyo ya moja kwa moja dhidi ya watetezi (kama vile mashirika binafsi ya vyombo vya habari na vya serikali pia). Vyote vinategemea mazingira na maslahi na mikakati ya kila mmoja wa wadau hawa muhimu. Orodha isiyo kamilifu inaweza kujumuisha:

- Taasisi za Umoja wa Mataifa (isipokuwa zile zilivyopewa mamlaka).
- Kamati ya Kimataifa ya Msalaba Mwekundu (ICRC).

- Serikali nyinginezo na taasisi za kimataifa (wafadhili na watunga sera).
- Watendaji wengine waliowezeshwa.
- Mashirika yasiyo ya kiserikali (kitaifa au kimataifa).
- Makanisa na taasisi za kidini.
- Mashirika binafsi.
- Vyombo vya habari.

Ugumu mkubwa kwa kuanzisha mikakati na vitendo ambavyo vinafanywa na wadau ni kwamba mahusiano kati yao hayatambuliki, au huenda hata kuwa hayapo. Washiriki wengi wenye wajibu, hususan serikali, vikosi vya usalama na makundi ya uasi, kusababisha au kuchangia katika ukiukwaji wa haki za binadamu na ukosefu wa ulinzi kwa watetezi. Baadhi ya wadau, ambao kwa namna moja pia wangeweza kushirikiana na masuala ya ulinzi huo, wanaweza kwa namna nyingine pia kuwa miongoni mwa serikali nyinginezo, vyombo vya vya Umoja wa Mataifa na mashirika yasiyo ya kiserikali (NGOs). Sababu hizi, pamoja na wale wanaohusika na matukio ya migogoro, mradi, mazingira magumu ya ufanyaji kazi kwa ujumla.

Kuna njia kadhaa za kufanya uchambuzi wa wadau. Hii ni yakutumia mbinu moja kwa moja, ambayo ni muhimu kwa kupata matokeo mazuri katika uchambuzi na taratibu za ufanyaji wa maamuzi.

Wakati wa kuchunguza mbinu za ulinzi na usalama ni muhimu kuzitazama kwa kina na daima kuzingatia maslahi na malengo ya wadau wote waliohusika.

(h) Kuchambua miundo na taratibu zibadilikazo

Wadau si watendaji wasiobadilika. Wao huhusiana na kila ngazi katika viwango vingi, na kuunda mtandao wa mahusiano. Kwa upande wa ulinzi, ni muhimu kuonyesha na kuzingatia uhusiano unaojenga na kubadilisha mahitaji ya ulinzi wa watu. Tunaweza kuzungumzia juu ya miundo na michakato.

Miundo inahusiana na sekta ya umma, mashirika ya kiraia au vyombo binafsi. Tutawaangalia kutoka kimtazamo wa ulinzi. Katika sekta ya umma, tunaweza kuangalia serikali kama seti ya watendaji ambao ama wana mkakati mmoja unganifu au kwa kukabiliana na mikakati ya ndani. Kwa mfano, tunaweza kupata tofauti kati ya Wizara ya Ulinzi na Wizara ya Mambo ya Nje wakati wa kujadili sera zinazohusiana na watetezi wa haki za binadamu, au kati ya ofisi ya Kamishna wa Utawala Bora na Haki za Binadamu (Ombudsman) na jeshi. Miundo inaweza kuwa na sehemu zilizochanganywa; kwa mfano, tume mseto kisekta (wanachama kutoka serikalini, mashirika yasiyo ya kiserikali, mashirika ya Umoja wa Mataifa na kidiplomasia) ingeliweza kuundwa kufuatilia ili hali ya ulinzi wa shirika husika la watetezi wa haki za binadamu.

Mchakato ni muunganiko wa pande nyingi za maamuzi na hatua zilizochukuliwa na muundo mmoja au zaidi wenye lengo la kuboresha hali ya ulinzi wa kundi fulani. Kunaweza kuwa na taratibu za kisheria, taratibu za kitamaduni na michakato ya sera. Sio michakato yote hufanikiwa katika kufanikisha maboresho katika ulinzi: Mara nyingi michakato ya ulinzi inakinzana au mchakato mmoja husababisha mwingine kudhorota. Kwa mfano, watu wanaodaiwa kuwa wanalindwa hawawezi kukubaliana na mchakato wa sera ya ulinzi unaongozwa na serikali, kwa sababu wanaiona sera hiyo kuwa na lengo la kuwaondoa kabisa watu kutoka eneo hilo. Umoja wa Mataifa na mashirika yasiyo ya kiserikali wanaweza kuwasaidia watu hawa katika mchakato huu.

(I) Uchambuzi wa wadau katika hatua nne:

1. Tambua kwa upana swala linalohitaji ulinzi i (yaani hali ya usalama ya watetezi wa haki za binadamu katika kanda husika ndani ya nchi).
2. Wapi ni wadau? (kwa kuwataja, ni taasisi na vikundi na watu binafsi wenye jukumu au maslahi katika ulinzi?) Tambua na uorodheshe wadau wote wanaohusika na suala hilo la ulinzi, kwa njia ya mawazo na majadiliano.
3. Kuchunguza na kuchambua sifa za wadau na sifa fulani, kama vile majukumu katika ulinzi, uwezo wa kuathiri mazingira ya ulinzi, lengo, mikakati, uhalali na maslahi (ikiwa ni pamoja na nia ya kuchangia kwenye ulinzi).
4. Kuchunguza na kuchambua mahusiano kati ya wadau.

Baada ya kufanya uchambuzi huu, unaweza kutumia majedwali kama ifuatavyo

Weka orodha na wadau wote wanaohusika na suala la kulindwa vizuri katika jedwali (tazama chati 2): Rudia orodha sawa katika safu ya kwanza pande zote. Baada ya hapo, unaweza kufanya aina mbili za uchambuzi:

- Kuchambua sifa za kila wadau (malengo na maslahi, mikakati, uhalali na nguvu), kujaza masanduku kwenye mstari wa unaounganisha pande mbili ambapo kila mdau hujiunga. Kwa mfano:
- Unaweza kuweka malengo na maslahi na mikakati ya vikundi vya uasi vyenye silaha katika kisanduku “A”.
- Kuchambua mahusiano kati ya wadau, kujaza katika visanduku ambavyo vinafafanua mahusiano muhimu zaidi kuhusiana na suala la ulinzi, kwa mfano, moja wapo inayoingilia kati ya jeshi na Kamishna Mkuu wa Umoja wa Mataifaanayeshughulikia masualaWakimbizi (UNHCR), katika kisanduku “B “, Nakadhalika.

Baada ya kujaza visanduku muhimu zaidi, utakuwa na picha ya malengo na mikakati na mwingiliano miongoni mwa wadau wakuu kuhusiana na suala la ulinzi husika.

Sura ya

3

Kutathmini Hatari

3.0 Utangulizi

Hatari inaweza kuelezewa kama uwezekano wa tukio ambalo husababisha madhara. Hatari inaweza kuwa matukio mabaya yanyowakabiri watetezi wa haki za binadamu (HRDs) katika kazi zao za kila siku. Kazi za watetezi wa haki za binadamu zinaweza kuwa na athari hasi kwa maslahi ya watendaji muhimu na hii inaweza kuwaweka watetezi hatarini. Kwa hiyo ni muhimu kusisitiza kwamba hatari ni sehemu ya asili ya maisha ya watetezi katika nchi fulani. Hatari hii huweza luwakumba wao, familia zao, mashirika, na watu wanaowakilisha katika matukio hatarishi.

3.1 Sababu zinazochangia kuongezezeka kwa kiwango cha Hatari kwa Watetezi wa Haki za Binadamu

a. Mazingira ya kisiasa

Mazingira ya kisiasa ambamo watetezi wa haki za binadamu hufanya kazi yana ushawishi wa moja kwa moja juu ya kiwango cha hatari wanazokabiliana nazo. Kwa mfano, vipindi vya uchaguzi katika baadhi ya maeneo ya nchi ni kawaida na huwakilisha kipindi kigumu na hatarishi.

b. Teknolojia

Karne ya 21 kumeshuhudiwa kukua na kubadilika kwa teknolojia kwa ufanisi, ambayo imeimarisha sana uwezekano wa kudhuru watetezi wa haki za binadamu . Mawasiliano kati ya watetezi, nchi, na mabara yameongezeka, lakini mabadiliko ya habari kwenda kwenye dijitali pia umesababisha udhaifu zaidi. Hivi vinatoka kwenye njia zilizoathiriwa za mawasiliano na ufuatiliaji, uingiliaji, udukuzi wa habari, na uzuiaji wa habari kupitia miundombinu ya kidijitali. Hata wakati ambapo hatua zimechukuliwa ili kuanzisha mifumo salama, kumekuwa na matukio ambapo wavamizi au wahusika wameweza kupunguza au kupitisha mifumo.

c. Mandhari ya utetezi

Kazi ya haki za binadamu mara kadhaa huonekana kwa watendaji wa mamlaka za serikali na wasio wa serikali kama kazi iliyopangwa kuangamiza na kuingilia hali fulani iliyopo ya nchi husika. Kuna masuala kadhaa ya kimandhari kwa watetezi yanayoweza sababisha changamoto zaidi kwa watetezi. Masuala haya ni pamoja na haki za wazawa na wafugaji, haki za wanawake na haki za kijinsia, haki za kiraia na kisiasa, na haki za mazingira.

3.2 Tathmini ya Hatari

Wakati wa tathmini ya hatari, watetezi wanahitaji kutambua na kutathmini viashiria vya hatari. Wanaweza kutambua uwezekano na athari za hatari zinazohusiana na vitisho.

Suala la hatari linaweza kutathminiwa kwa njia ifuatayo:

- Kuchambua maslahi na mikakati ya wadau wa msingi
- Kutathmini matokeo ya kazi za watetezi juu ya maslahi na mikakati hiyo
- Kutathmini tishio dhidi ya watetezi
- Kutathmini udhaifu na uwezo wa watetezi
- Kuionesha Hatari iliyopo kwa watetezi

Kwa muhtasari, tathmini za hatari zinahusisha kutathmini vitisho, udhaifu, na uwezo. Haya ni mambo yanayochangia kuongeza viwango vya hatari kwa watetezi wa haki za binadamu .

Vitisho

Hivi ni viashiria au uwezekano wa kuwa mtu atamdhuru kimwili au wa kimaadili au kuathiri kitu fulani kwa njia ya vurugu za makusudi . Watetezi wanaweza kukabiliana na vitisho vingi tofauti katika hali ya mgogoro, ikiwa ni pamoja na kulenga, uhalifu wa kawaida na vitisho vya moja kwa moja. Aina ya kawaida ya tishio inayolenga kuzuia au kubadilisha kazi ya kikundi, au kuathiri tabia ya watu wanaohusika. Ulengaji kawaida huhusiana sana na kazi iliyofanywa na watetezi katika kuhoji. Pamoja na maslahi na mahitaji ya watu wanaopinga kazi ya watetezi.

Udhaifu

Udhaifu unaweza kuelezwa kama mapungufu waliyonayo watetezi wa haki za binadamu ambayo huongeza uwezekano wa madhara au kuongezeka kwa athari zake: kama vile ambavyo ua lenye rangi na harufu nzuri ambavyo hulifanya kushambuliwa na wadudu. Hata viashiria ambavyo watetezi huwanavyo au vinavyowazunguka na hata matendo ambayo mtetezi hufanya au hafanyi vingeliweza kumsababishia athari.

Vielelezo vingine juu ya udhaifu;

Udhaifu unaweza kuwa juu ya eneo: Kawaida mtetezi huwa katika udhaifu zaidi katika mazingira magumu wakati yeye akiwa nje ya ziara kwenye eneo husika yeye akiwa katika ofisi inayojulikana ambapo mashambulizi yoyote yanaweza kushuhudiwa.

Udhaifu unaweza kuhusisha ukosefu wa upatikanaji wa simu, usafiri salama wa nchi kavu au kukosekana kwa kufuli zuri kwenye milango ya nyumba. Lakini mazingira magumu yanahusiana pia na ukosefu wa mitandao na mwitikio shirikishi miongoni mwa watetezi.

Udhaifu unaweza pia kutokuwa na ushirikiano wa timu yenye kufanya kazi pamoja na pia kuwa na hofu: mtetezi anayepata tishio anaweza kuogopa, na kazi yake huweza kuathiriwa na hofu. Ikiwa hawana njia sahihi ya kukabiliana na hofu (mtu mmojawapo kuzungumza timu nzuri ya wenzake, nk) nafasi ni kwamba, yeye anaweza kufanya makosa au kuchukua maamuzi maskini ambayo yanaweza kumsababisha matatizo zaidi ya usalama.

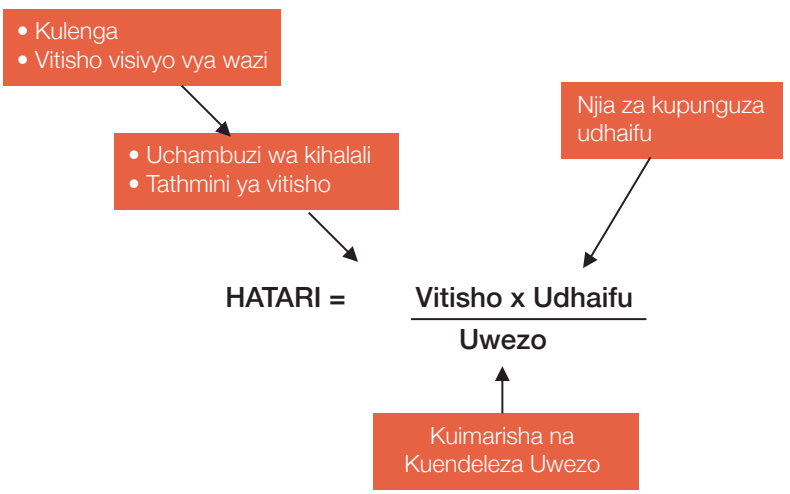
c. Uwezo

Katika mahusiano na udhaifu, uwezo ni rasilimali, uwezo, na nguvu ambazo zinaweza kutumika kupunguza madhara na athari zake: sawa na kutumia bakuli la sukari yenye kifuniko cha kushika ili kuondoa sungusungu. Mifano ya uwezo inaweza kuwa mafunzo katika masuala ya usalama au kisheria, kikundi kinachofanya kazi pamoja kama timu, upatikanaji wa simu na usafiri salama, kwenye mitandao mizuri ya watetezi, kwa mkakati sahihi wa kukabiliana na hofu, nk.

Kwa hiyo;

Ili kupunguza hatari kwa viwango vinavyokubalika –haina budi:

- Kupunguza vitisho.
- Kupunguza sababu za udhaifu.
- Kuongeza uwezo wa kujilinda.



Mchoro hapo juu unaonesha kanuni ya kukokotoa Hatari

Hatari ni dhana inayobadilika kulingana na muda tofauti mbalimbali katika hali ya vitisho, udhaifu na uwezo. Hii inamaanisha hatari lazima itathminike katika kipindi maalum, hasa ikiwa mazingira yako ya kazi, vitisho au udhaifu kubadilika. Kwa mfano, udhaifu unaweza kuongezeka ikiwa mabadiliko ya uongozi huwaacha kundi la watetezi kwa nafasi dhaifu kuliko hapo awali. Hali ya hatari huongezeka sana kwa tishio lililo wazi na halisi. Katika hali hiyo, hakuna salama katika kujaribu kupunguza hatari kwa kuongeza uwezo, kwa sababu hiyo inachukua muda.

Hatua za usalama, kama vile mafunzo ya kisheria au kinga za kuzuia, vinaweza kupunguza hatari kwa kupunguza sababu za mazingira magumu. Hata hivyo, hatua hizo hazipati chanzo kikuu cha hatari, yaani, vitisho, wala niya ya kutekeleza, hasa katika hali ambapo wahalifu wanajua kuwa wanaweza kwenda bila kuadhibiwa. Hatua zote muhimu katika ulinzi zinapaswa kupunguza vitisho, pamoja na kupunguza udhaifu na kuimarisha uwezo.

Mfano

Kikundi kidogo cha watetezi wanaofanya kazi katika masuala ya rasilimali ardhi katika mji. Mara kazi yao inapoanza kuathiri maslahi ya wamiliki wa ardhi, wanapata tishio la wazi la kifo. Ikiwa unatumia usawa wa tishio kwa hali yao ya usalama, utaona kwamba hatari inayowakumba watetezi ipo juu sana kuzidi zingine kutokana na tishio la kifo.

Ikiwa unataka kupunguza hatari hiyo labda sio wakati wa kuanza kubadili kufuli kwenye mlango wa ofisi zao (kwa sababu hatari haihusiani na kuvunja na kuingia katika ofisi), wala wakati wa kununua simu ya mkononi kwa kila mtetezi (hata kama mawasiliano yanaweza kuwa muhimu kwa usalama haitoshi kama kuna mtu anakuja kukuua).

Katika kesi hii, mkakati unaofaa zaidi ni kufanya kazi kwenye mitandao na kuibua mwitiko wa kisiasa katika kushughulikia moja kwa moja tishio (na kama haiwezekani kuwa na ufanisi haraka njia pekee ya kupunguza hatari kwa kiasi kikubwa inaweza kuwa kupunguza mwonekano wa wazi kwa watetezi katika eneo lile, labda kwa kuwahamisha kwa muda kwenda maeneo salama pia nao ni uwezo).

Kufanya na kutekeleza uamuzi huo pia unahusisha uwezo wa kisaikolojia kwa mtetezi kuona kwamba uondolewaji sio sawa na hofu au kushindwa. Kuondolewa kunaweza kuruhusu kutafakari na kurudia kazi mara nyingine kwa uwezo Zaidi.

3.3 Makosa ya kawaida kuhusu uchambuzi wa hatari kwa watetezi

Kuzingatia mikakati mwitikio: watetezi wengi wa haki za binadamu huweka tu hatua za usimamizi wa usalama baada ya kukabiliwa na hatari au vitisho. Tathmini ya hatari hizo husaidia kupunguza athari kwa watetezi na kazi zao. Kwa kufanya tathmini, watetezi wanaweza kupanga mikakati ya kuzuia hatari kama hizo na kushughulikia kwa njia salama.

Njia ya kunukuu na kunakili: watetezi wengine hutumia hatua za udhibiti wa usalama ambazo zinafanya kazi kwa watetezi wengine. Watetezi hufanya kazi kwenye mandhari tofauti na hufanya kazi kwa mazingira tofauti, kwa hiyo hali ya kuimarisha hatua za usalama. Kwa mfano, ufungaji wa kamera za CCTV zinaweza kuvuta umakini na juu ya tuhuma kwa watetezi wanaofanya kazi maeneo ya vijijini

Ushujaa: Wakati mwingine ujasiri huwaweka watetezi katika hatari zisizo za lazima. Inashauriwa kwamba, watezizi wapime udhaifu wao dhidi ya vitisho ama hofu inayowakabiri.

Uelewa mbaya wa kazi za watetezi wa haki za binadamu. Katika hali nyingine, watetezi huchanganya uanaharakati wa kisiasa na shughuli za utetezi wa haki za binadamu, ambazo zinaweza kuzua mjadala kati ya mamlaka na Asasi za kiraia. Majadiliano mazuri yanayojumuisha pande mbili hutengeneza tuhuma angali bado serikali na watetezi wanapaswa kufanya kazi kwa usaidizi

Kasumba ya kupuuza usalama wa mtu: katika baadhi ya matukio, watetezi huwa wanatoa kipaumbele zaidi kwa kazi zao na waathirika wa ukiukwaji. Msingi wa kazi ya za watetezi wa haki za binadamu umejikita katika usalama wao na bila kazi ya haki za binadamu haiwezi kudumishwa

Sura ya

4

Kuelewa na Kutathmini Vitisho

4.0 Utangulizi

Tishio kwa Watetezi wa Haki za Binadamu linaweza kuelezewa kama “dhamira au dalili ya nia ya kudhuru, kuadhibu au kuumiza”. ‘Vitisho vinatumiwa sana ili kuwafanya watetezi wajione dhaifu, kuwa na wasiwasi, kumechanganyikiwa na kujihisi hawana msaada. Watetezi wa haki za binadamu wanapata vitisho kwa sababu ya athari ya kazi zao. Pia vitisho vingi vina lengo la kumfanya mtetezi aache kazi yake au kumlazimisha mtetezi atomize matakwa ya anayemtisha.

Vitisho huashiria uwezekano wa mtu mmoja kumdhuru mtu mwingine kimwili au kimaadili au kuharibu mali za mtu mwingine makusudi na kwa ghasia. Watetezi wanaweza kukabiliana na aina nyingi za vitisho katika mazingira ya migogoro, ikiwa ni pamoja vitisho vya kuwalenga watetezi, uhalifu wa kawaida dhidi ya watetezi na vitisho visivyo vya moja kwa moja.

Aina nyingi za vitisho zipo kama ifuatavyo;

- Ulengaji – Hivi ni vitisho vya mashambulio dhidi ya watetezi vinavyolenga kuzuia au kumlazimisha mtetezi au kikundi cha watetezi kuacha kazi yake ya utetezi au kuathiri tabia za watu wanaohusika na utetezi. Ulengaji kikawaida huhusiana sana na kazi zinazofanywa na watetezi husika, pamoja na maslahi na mahitaji ya watu wanaopinga kazi za watetezi.
- Tishio la mashambulizi ya kawaida ya jinai – Vitisho hivi hasa huhusiana na kazi za watetezi zinazowaweka katika maeneo hatarishi. Matukio mengi ya kulengwa yanafanyika kwa mtizamo wa kwamba ni “matukio ya kawaida” tu ya jinai.
- Vitisho visivyo vya moja kwa moja – Hutokea kutokana na madhara yanayosababishwa na mapigano ya kivita au ghasia, kama vile “kuwa sehemu ya hatari, wakati mbaya”. Hii hutokea hasa kwa watetezi wanaofanya kazi katika maeneo yenye vita.
- Vitisho vya matamko - kwa mfano kupokea tishio la kuuawa.

4.1 Vipengele vya Tishio

- Chanzo; Mfano mtu au kikundi cha watu ambao wameathirika na kazi ya mtetezi na kisha kutoa tishio.
- Lengo la tishio ambalo linahusishwa na athari za kazi ya mtetezi, na
- Njia iliyotumika; yaani jinsi tishio lilivyowasilishwa kwa mtetezi.

Vitisho ni mitego. Tunaweza kusema kwa kiasi fulani cha kejeri kuwa vitisho ni vya “kiikolojia”, kwa sababu vinalenga kufikia matokeo makubwa kwa uwekezaji wa nguvu kidogo. Mtu anayetoa kitisho amechagua kufanya hivyo, kuliko kuchukua hatua moja kwa moja - uwekezaji mkubwa wa nguvu. Lakini tujiulize, Kwa nini? Kunaweza kuwa na sababu kadhaa, na ni muhimu kuzitaja hapa:

- Mtu anayetoa vitisho ana uwezo wa kutekeleza vitisho lakini kwa kiasi fulani huogopa gharama za kisiasa zitazomkabili kwa kutekeleza vitisho waziwazi dhidi ya mtetezi wa haki za binadamu. Vivyo hivyo, vitisho vinavyotolewa na watu wasojulikana, vinaweza kutolewa kwa sababu hizohizo.
- Mtu anayetoa vitisho ana uwezo mdogo wa kuvitekeleza lakini anataka kufanikisha lengo lake kwa kuficha uwezo wake mdogo nyuma ya vitisho. Uwezo huu mdogo unaweza kuwa wa muda tu kutokana na vipaumbele vingine, au unaweza pia kudumu na kubaki mdogo. Lakini katika hali zote mbili, mambo yanaweza kubadilika muda wowote na kusababisha madhara ya moja kwa moja dhidi ya mtetezi baadaye.

4.2 Vitisho na Watetezi wa Haki za Binadamu nchini Tanzania

Kama watetezi wengine wa haki za binadamu kwingineko duniani, watetezi nchini Tanzania pia wanakabiliwa na vitisho. Vitisho vinavyotokana na mamlaka husika zinazotishia kuyafutia usajili mashirika yasiyo ya kiserikali, vimejitokeza sana hasa kwa watetezi wanaofanya kazi za utetezi wa haki za wafugaji huko Wilayani Loliondo (NGONET na PINGOs Forum). Mnamo mwaka 2017, viliibuka vitisho vya kukifutia usajili Chama cha Mawakili Tanganyika (TLS) kilichoshutumiwa kujihusisha na harakati za kisiasa.

Katika hotuba ya Juni 22, 2017, Rais Magufuli alitoa katazo la utoaji wa huduma ya elimu bure kwa wasichana wanaopata ujauzito wakiwa shuleni. Alidai kuwa hakubaliani na msimamo wa mashirika yasiyo ya kiserikali yanayolaani uvunjaji wa haki ya elimu kwa watoto.

Rais alisema kuwa “kwa muda ambao mimi nitakuwa rais, hakuna wanafunzi wajawazito wataruhusiwa kurudi shule”. Siku tatu baadaye, katika mkutano jijini Dodoma, aliyekuwa Waziri wa Mambo ya Ndani Mhe. Mwigulu Nchemba pia aliyatishia mashirika ambayo yanapinga na kwenda kinyume na katazo hilo la Rais. Baadaye, Chama cha Wanawake Wanasheria (TAWLA) kilionywa kuhusu kuziongoza AZAKi zingine kwenye suala hilo la elimu kwa wasichana wanaopata ujauzito wakiwa shuleni.

4.3 Tathmini ya Vitisho

Mwisho wa siku, tunahitaji kujua kama tishio linaweza kutekelezwa au la. Ukiwa una hakika kwamba tishio hili haliwezekani kutekelezwa na mhusika, utakabiliana nalo tofauti kabisa na ikiwa una uhakika tishio husika linaweza kutekelezwa.

Malengo makuu mawili wakati wa kutathmini tishio ni:

Ili kupata habari nyingi iwezekanavyo kuhusu madhumuni na chanzo cha vitisho (vyote viwili vitakuwa vinahusishwa na athari za kazi zako za utetezi).

Ili kufikia maamuzi kama tishio litatekelezwa au la.

4.4 Hatua tano za kutathmini kitisho

Kubaini ukweli halisi juu ya tishio/vitisho. Ni muhimu kujua hasa kilichotokea. Hii inaweza kufanyika kupitia mahojiano au kwa kuuliza maswali kwa watu muhimu, na mara moja moja kupitia ripoti husika.

Kubaini kama kuna mfululizo wa vitisho vinavyohusiana katika kipindi husika. Ikiwa vitisho kadhaa vinatolewa mfululizo (kama ilivyo kawaida) ni muhimu kuangalia uhusiano wa kila kitisho, kama vile njia zinazotumiwa kutoa vitisho, nyakati ambazo vitisho vinaonekana, alama, taarifa zinazotolewa kwa maandishi au maneno, nk. Si rahisi kubaini uhusiano wa vitisho, lakini ni muhimu kwa kufanya tathmini sahihi ya vitisho hivyo.

Kubaini lengo la tishio. Kwa kawaida tishio huwa na lengo linalohusishwa na mlolongo wa athari za kazi za mtetezi kwa wahusika, unaoweza kubaini dhumuni au lengo la tishio husika.

Kumbaini anayetoa vitisho. (Hili linaweza kufanyika kwa kupitia hatua tatu za mwanzo kwanza). Jaribu kuchanganua kwa kina kadri iwezekanavyo. Kwa mfano, unaweza kusema kwamba “serikali” inakutisha. Lakini kwasababu serikali ni mjumuiko wa watendaji wengi, hivyo basi ni muhimu zaidi kujua ni sehemu gani ya serikali inaweza kuwa nyuma ya vitisho. Wafanyakazi kama vile “vikosi vya usalama” na “vikundi vya waasi” pia ni watendaji walio ndani ya mjumuiko huo. Kumbuka kwamba hata tishio lililosainiwa laweza kuwa la uwongo. Hii inaweza kuwa mbinu mbadala ya mtu anayetoa vitisho kwa siri kuepuka gharama za kisiasa na bado kufikia lengo lake la kuwatia hofu watetezi wa haki za binadamu na kujaribu kuwazuia kufanya kazi zao.

Fikia maamuzi ya busara kuhusu uhalisia wa utekelezwaji wa tishio kama linaweza kutekelezwa au la. Hatari ya tishio hutegemea mazingira husika. Huwezi kamwe kuwa na uhakika kabisa kuwa tishio litatekelezwa ama la. Kufanya utabiri kuhusu utekelezwaji wa tishio kutategemeana na hali ya hatari iliyopo itakayosababisha wahusika/mhusika kutekeleza tishio kwa mtetezi.

Sura ya

5

Matukio ya Kiusalama

5.0 Utangulizi

Tukio la kiusalama ni tukio lolote ambalo linaweza kuwaweka watetezi wa haki za binadamu (HRDs) au mashirika yao hatarini. Matukio ya kiusalama hutoa fundisho kwa watetezi na mashirika yao juu ya athari za kazi zao na jinsi maslahi ya watu mbalimbali yanavyoathirika. Pia huwapa fursa watetezi na mashirika yao kupitia upya mifumo na taratibu zao za ulinzi na usalama.

Mifano ya matukio ya usalama:

Wakati mwingine wapelelezi hutumwa kwenye ofisi za watetezi wa haki za binadamu ili kujua muda ambao watetezi huingia na kutoka ofisini, usafiri wanaotumia, rangi za gari zao, na kadhalika.

- Uvujaji wa taarifa juu ya kesi nyeti inaweza kusababisha vitisho vya kiusalama kama vile kukamatwa na kuwekwa kizuizini, kufwatiliwa na kutishiwa na mtu anayehusika katika ukiukwaji wa haki za binadamu.
- Ikiwa wageni hawakaguliwi vizuri na vitambulisho vyao havirekodiwi, mtu yeyote anaweza kuingia katika ofisi za watetezi na kufanya uhalifu au kuathiri usalama wao. Kukosekana kwa ushahidi wa ugeni dhidi ya wahusika, kisheria kunaweza kusababisha wasiadhibiwe.

'Tukio la kiusalama ni "kiashiria cha kidogo sana" katika kupima hali ya usalama na pia huashiria upinzani/shinikizo juu ya kazi yako kama Mtetezi wa Haki za Binadamu. Usiache matukio ya kiusalama yapite bila kutambuliwa!'

5.1 Hali ya watetezi wa haki za binadamu (HRDs) nchini Tanzania

Kama itakavyoelezwa hapa chini, kuyatambua matukio ya kiusalama kunahitaji ufahamu juu ya dhana ya ulinzi na usalama kwa watetezi wa haki za binadamu. Kwa kawaida, watetezi wengi wa haki za binadamu ambao hawazifahamu kanuni za ulinzi na usalama huyachukulia matukio ya kiusalama kimzaha na hawawezi kuyachambua.

Tanzania kwa mfano, wakati wa kuanzishwa kwa Mtandao wa Watetezi wa Haki za Binadamu Tanzania (THRDC), watetezi wachache sana walikuwa na ujuzi wa masuala ya ulinzi na usalama. Kulingana na tafiti THRDC ya mawaka 2013 juu ya tathmini ya mahitaji ya watetezi nchini, watetezi 135 tu kati ya 2000 kutoka mashirika ya haki za binadamu na vyombo vya habari walikuwa wameshawahi kuhudhuria mafunzo ya usalama kwa watetezi, aidha nchini au nje ya Tanzania.

Kuanzishwa kwa THRDC hususani dawati lake la ujengaji uwezo na uwezeshaji, umefumbua macho ya watetezi wengi kupitia mafunzo ya usalama na wameweza kutambua asili ya mazingira yao ya kazi, hivyo ni rahisi kwao kuyatambua na kuyakabili matukio ya kiusalama dhidi yao.

Kwa mfano haya hapa ni baadhi ya matukio yaliyoripotiwa ya usalama yaliyotajwa na watetezi waliopata mafunzo;

- Ndugu Deus Kibamba (Mkurugenzi Mtendaji wa zamani, Jukwaa la Katiba)

  Mnamo tarehe 12 Aprili 2013, kati ya saa 5 asubuhi hadi saa 6 mchana, gari aina ya Land Cruiser lenye rangi ya bluu, lenye na namba za usajili T126 CCG, lilionekana likiwa limepaki kwenye eneo la ofisi za Jukwaa la Katiba, likiwa na watu sita ndani, ambapo wawili kati yao walielekea geti kuu la ofisi hiyo kumuulizia Mkurugenzi Mtendaji wa Jukwaa la Katiba Ndugu Deus Kibamba pamoja na Mratibu wake Bi. Diana Kidala. Wawili hawa walijifanya kuwa na undugu na Bwana Kibamba. Cha kushangaza, waliomba pia namba zake za simu baada ya kutambua kwamba wamegonga mwamba. Baadae, wawili hawa walionekana wakijadiliana nje ya ofisi za Jukwaa la Katiba kwa muda wa takribani lisaa limoja. Jukwaa la Katiba iliripoti tukio hilo la kiusalama kwa Jeshi la Polisi na wakati huohuo THRDC ilitoa tamko kwa vyombo vya habari kulaani tukio hilo na kuchukua hatua za kulifanyia tukio hilo uchunguzi.

- Ndugu Antony Lyamuda, Mkurugenzi Mtendaji wa Civil Education is the Solution to Poverty and Environmental Management (CESOPE)

  Mnamo mwezi Machi 2013, Bw. Lyamunda alipokea vitisho na kufwatiliwa mara kwa mara na watu wasiojulikana. Katika jitihada za kuyakabili matukio haya ya kiusalama, Bw. Lyamunda alisaidiwa kwa kuondolewa nje ya nchi kwa muda.

- Ndugu Maxence Melo, Mkurugenzi Mtendaji wa Jamii Media (JamiiForums); kama moja wapo ya tovuti zinazotumiwa na watumiaji mitandaoni kuandika, kujadili na kufuatilia masuala mbalimbali ya muhimu katika jamii. Aliripoti vitisho na matukio kadhaa ya kiusalama dhidi yake kwa Mtandao wa Watetezi wa Haki za Binadamu Tanzania (THRDC), ambapo matukio haya yalijumuisha zaidi ya barua tano alizoandikiwa na jeshi la polisi mnamo mwaka 2016, akitakiwa kufichua anwani za IP za baadhi ya watumiaji wa JamiiForums. Jeshi la polisi lilimshtaki kupitia kifungu namba 32 cha Sheria ya Makosa ya Mtandao ya mwaka 2015.

- Ndugu Onesmo Olengurumwa, Mratibu Kitaifa wa Mtandao wa Watetezi wa Haki za Binadamu Tanzania (THRDC)

  Kati ya mwaka 2017 na mwaka 2018, Bw. Onesmo Olengurumwa alihojiwa mara kadhaa kuhusu utaifa wake kutokana na kazi yake ya utetezi wa haki za binadamu. Alikamatwa na kushtakiwa mwaka 2017 wakati wa uzinduzi wa kitabu cha mtetezi kijana Alphonce Lusako. Watu wasiojulikana walionekana maeneo ya nyumbani kwake wakati yeye hayupo wakiwauliza watoto wake kuhusu mahali alipo baba yao.

5.2 Jinsi ya Kukabiliana na Matukio ya Kiusalama

Athari za kazi za watetezi wa haki za binadamu, mara nyingi zinaweza kupimwa kupitia mtazamo wa jamii yao. Wakati tukio la kiusalama linapotokea, mtetezi anapaswa kuchukua hatua kadhaa ili kuhakikisha kwamba tukio hilo linashughulikiwa vizuri. Hatua hizi zinaweza kutofautiana kwa matukio tofauti.

Hatua ya 1: Kuripoti Tukio

Mtetezi wa Haki za Binadamu anapopata tukio la kiusalama, anapaswa kuripoti au kutoa taarifa ya tukio husika kwa mtu maalumu anayesimamia masuala ya usalama katika shirika lake au kwa mkurugenzi wa shirika lake. Wanachama wa Mtandao wa Watetezi wa Haki za Binadamu (THRDC) pia wanaweza kuripoti moja kwa moja kwa Afisa Ulinzi na Usalama wa THRDC katika makao makuu ya THRDC.

Taarifa muhimu katika ripoti hii inapaswa kujumuisha:

- Ni nani anayeripoti?
- Nini kimetokea? Kilitokea wapi? Kilitokea lini? (toa maelezo sahihi na ya kina kadri iwezekanavyo);
- Ni nani aliyehusika, na maelezo gani yametolewa na waathirika wa tukio hilo?;
- Nini athari ni juu ya wale walioathirika, na maelezo ya hali yao ya sasa;
- Ni nani aliyefanya tukio hilo, elezea kwa ufupi idadi, aina ya silaha, msaada wa awali uliotolewa, matukio ya baada ya tukio la kiusalama;
- Muhtasari wa hali ya muda huo na ikiwa bado kuna matatizo au la;
- Ikiwa ndio, ni maamuzi gani na hatua gani zimechukuliwa/zimependekezwa na aliyeripoti katika kukabili tukio la kiusalama.

Kumbuka: Ripoti ya tukio la kiusalama inaweza kuwa katika maandishi au maneno. Hata hivyo, tukio hilo linapaswa kuwekwa katika maandishi ili kuzuia kupoteza ukweli.

Hatua ya 2: Kuchunguza Ukweli

Wakati wa kuchunguza ukweli, masuala kadhaa yanahitaji kuzingatiwa: Ni nani atakuwa kahusika?, Ni wapi tukio la kiusalama lilitokea?, Kuna yeyote aliyejeruhiwa au mali iliyoharibiwa?, Ni nini lengo la wahusika?. Haya masuala yataamua hatua za kuchukua katika kukabiliana na tukio la kiusalama. Kufikia hapo, unapaswa kujua uzito wa tukio husika ili kujua kama tukio hilo ni dogo au kubwa.

Hatua ya 3: Kukabili au Kutokabili Tukio la Kiusalama

Uchunguzi unapoonesha kuwa tukio la kiusalama ni kubwa, watetezi wa haki za binadamu wanapaswa kuchukua hatua stahiki. Hatua ya kuchukua hutegemeana na hali ya tukio husika la kiusalama. Ikitokea ofisi imevamiwa, vitasa vipya na mifumo ya usalama inapaswa kuwekwa. Ikiwa tukio la kiusalama litachukuliwa kuwa la kawaida, watetezi wanaweza wasichukue hatua kubwa lakini wanapaswa kulirekodi tukio hilo kwa ajili ya marejeo baadaye.

Sura ya

6

Kuzuia na Kukabiliana na Mashambulizi

6.1 Utangulizi

Kushambulia ni mchakato, pia ni kitendo. Unapofanya uchambuzi vizuri wa mashambulizi mara nyingi utagundua kwamba shambulio ni hitimisho la migogoro, vitisho na makosa ambayo yamekuwepo tangu muda mrefu.

Mashambulizi dhidi ya Watetezi wa Haki za Binadamu ni matokeo ya angalau sababu tatu zinazoshabihiana:

- Mshambuliaji binafsi. Mashambulizi dhidi ya Watetezi wa Haki za Binadamu mara nyingi ni matokeo ya michakato ya kimawazo na tabia ambazo tunaweza kuzielewa na kujifunza kutokana na mawazo au tabia hizo hata kama ni kinyume cha sheria. Muhusika atahitaji kuwekeza katika njia za kukusanya taarifa (matukio ya kiusalama) kuhusu Mtetezi wa Haki za Binadamu aliyelengwa.
- Misingi na vichocheo vinavyopelekea mshambuliaji kuona shambulizi kama chaguo. Watu wengi ambao wanawashambulia Watetezi wa Haki za Binadamu huona kushambulia kama njia ya kufikia lengo au 'kutatua tatizo'.
- Mazingira yanayopelekea mashambulizi kufanyika.

6.2 Hali kwa ufupi juu ya mashambulio kwa Watetezi wa Haki za Binadamu Tanzania.

Tofauti na miaka iliyopita, Tanzania hivi karibuni imeshuhudia kuongezeka kwa mashambulizi, upotevu na utekaji nyara wa Watetezi wa Haki za Binadamu na waandishi wa habari unatekelezwa na watu wasiojulikana. Kuzuia kwa mikutano ya ndani wa Watetezi wa Haki za Binadamu na kukamatwa kiholela kumeenea.

Katika miaka mitano ambayo Mtandao wa Watetezi wa Haki za Binadamu Tanzania umekuwa ukifanya kazi, waandishi wa habari, maafisa wa polisi na Watetezi wa Haki za Binadamu wengine wamekuwa waathirika wakubwa wa mashambulizi. Mwaka 2017 kwa mfano, ofisi tatu za wanasheria (makampuni ya wanasheria) zilivamiwa na moja kati ya hizi ni (Kampuni ya Mawakili ya IMMMA) iliyopigwa bomu na kusababisha hasara kubwa ya mali na hofu ndani ya taaluma ya sheria. Mnamo Septemba 2017 kulikuwa na mashambulizi ya mabaya kwa Mtetezi wa Haki za Binadamu na Rais wa Chama Cha Mawakili Tanganyika, Mheshimiwa. Tundu Lissu. Washambuliaji

wa Watetezi wa Haki za Binadamu tajwa hapo juu hawajawahi kutambuliwa, hawajakamatwa na kufikishwa mahakamani ili kukabiliana na mashtaka yanayowapasa.

6.3 Nani ni hatari kwa Watetezi wa Haki za Binadamu?

Kwa ujumla, ni yeyote anayefikiri kuwa kushambulia Mtetezi wa Haki za Binadamu ni njia sahihi au ya muhimu ili kufikia lengo.

6.4 Ufuatiliaji na namna ya Kukabiliana nao

Mashambulizi mengine yanatanguliwa na vitisho. Mengine sio. Hata hivyo, tabia ya watu wanaopanga mashambulizi ya vurugu mara nyingi huonyesha ishara za hila, kwa sababu wanahitaji kukusanya taarifa kuhusu wakati sahihi wa unyanyasaji, kupanga jinsi ya kufikia lengo lao, na jinsi ya kukwepa.

Ufuatiliaji wa Watetezi wa Haki za Binadamu hufanyika kwa kawaida mahali pa kazi, nyumbani au mahali ambapo wanependelea kuonekana. Mashambulizi hufanyika wakati wa hatari zaidi au wakati wa uwezo dhaifu wa Watetezi wa Haki za Binadamu. Mtu yeyote katika eneo lako, kama vile walinzi au wabeba mizigo katika majengo, wafanyabiashara wanaotembeza bidhaa karibu na mlango wa kuingia, watu katika magari ya karibu, wageni, nk, ni rahisi kuangalia mienendo yako.

Ufuatiliaji unaweza kutumika kwa madhumuni kadhaa

- Kufahamu shughuli gani zinazofanyika, wakati gani na pamoja na nani.
- Kutumia taarifa hizi baadaye ili kushambulia watu binafsi au mashirika.
- Kukusanya taarifa muhimu ili kutekeleza mashambulizi.
- Kukusanya taarifa kwa hatua za kisheria au unyanyasaji mwingine (bila madhara ya moja kwa moja).
- Kukutisha wewe, wafuasi wako au watu wengine wanaofanya kazi na wewe.

Kwa hiyo ni muhimu kuchunguza na kuchambua ishara yoyote inayoonyesha uwezekano wa mashambulizi (kukabiliana na ufuatiliaji). Hii inajumuisha:

- Kuchunguza kwa kiasi kikubwa wale ambao wanaweza wakawa wanakufwatilia
- Kutambua mienendo ya watu wa eneo lako na mabadiliko katika mtazamo wao
- Kumshirikisha mtu wa tatu unayemwamini kuwaangalia kwa niaba yako bila kuwafwata moja kwa moja au bila wao kujua
- Kabla ya kufika nyumbani unaweza kumuuliza mwanafamilia au jirani anayeaminika kuangalia kwa ukaribu na (kwa mfano. kubadilisha tairi la gari), ili uone kama kuna mtu anasubiri ufike.
- Kutambua na kuchambua matukio ya usalama
- Kutambua uwezekano wa tishio unaoweza kufanywa

Ni muhimu kutambua kwamba;

- Kushambulia mtetezi si rahisi na inahitaji rasilimali.

  Ufuatiliaji unahitajika ili kutambua harakati za mtu binafsi na eneo bora la kushambulia. Kufikia lengo na kutengeneza ufanisi, wa haraka pia ni muhimu. (Hata hivyo, kama mazingira yanafaa sana kwa mshambuliaji, mashambulizi ni rahisi kufanyika.)

- Watu ambao wanashambulia watetezi kawaida huonyesha kiwango cha uthabiti.

  Mashambulizi mengi yanalenga watetezi ambao wanahusika sana katika masuala yanayoathiri mashambulizi. Kwa maneno mengine, unyanyasaji haufanyiki ovyo ovyo au bila kusudi, bali hukidhi maslahi ya washambuliaji.

- Sababu za kijiografia

  Kwa mfano, mashambulizi dhidi ya watetezi katika maeneo ya vijijini yanaweza kuwa hayaufikii umma kwa kiasi kikubwa na hivyo kusababisha udhibiti mdogo wa watekelezaji wa sheria na ngazi ya kisiasa kuliko mashambulizi katika maeneo ya mijini. Mashambulizi dhidi ya makao makuu ya shirika au mashirika ya yenye sifa kubwa katika maeneo ya mijini huwa yanadhibitiwa zaidi.

- Chaguo na maamuzi hufanywa kabla ya kushambuliwa.

  Watu wanaopanga shambulio dhidi ya shirika la watetezi wanapaswa kuamua aidha kuwashambulia viongozi au wanachama wa ngazi ya chini, na kuchagua moja kati ya hao (dhidi ya muhusika mkuuna hivyo kupelekea kutumika kwa gharama kubwa kwa washambuliaji) au mfululizo wa mashambulizi (yanayoathiri uanachama wa shirika). Uchunguzi mdogo uliofanyika juu ya mashambulizi dhidi ya watetezi unaonyesha kwamba mikakati yote iliyotajwa hapo juu mara nyingi hutumika.

Sura ya

7

Kukamatwa, kuwekwa Kizuizini na Kushitakiwa kwa Mtetezi wa Haki za Binadamu

7.0 Utangulizi

Ni muhimu kutambua kwamba, kukamatwa, kuwekwa kizuizini na kushitakiwa kwa mtetezi au mtu mwingine yeyote kunaongozwa na sheria tofauti na vyombo tofauti vya utekelezaji wa sheria. Kwahiyo, Mtetezi wa Haki za Binadamu anahitaji kuwa na ufahamu mpana au kwa kifupi kuhusu haki zake wakati matukio yoyote yaliyotajwa hapo juu yanapotokea.

7.1 Hali ya kukamatwa, kuwekwa kizuizini na kushitakiwa kwa mtetezi

Hali ya kukamatwa, kuwekwa kizuizini na kushitakiwa kwa Watetezi wa Haki za Binadamu nchini Tanzania imeongezeka katika kipindi cha miaka miwili iliyopita. Hali hii imesababishwa ya matumizi mabaya ya nguvu, kutokujali, hali ya kisiasa, kutokuheshimu utawala wa sheria na utawala bora. Watetezi wa Haki za Binadamu wamekuwa kundi lililoathirika zaidi katika matukio haya. Mtandao wa Watetezi wa Haki za Binadamu Tanzania chini ya Dawati lake la Ulinzi la mwaka 2016 na 2017 liliweza kurekodi matukio zaidi ya 70 ya ukiukwaji wa haki za binadamu ikiwa ni pamoja na kukamatwa kiholela, kuwekwa kizuizini kinyume cha sheria, na mashtaka ya kughushi. Matukio haya sio tu kwamba yanakiuka haki ambazo watetezi wa haki za binadamu wamepewa lakini pia hufanya mazingira yao ya kazi kuwa mabaya zaidi.

7.1.1 Kukamatwa

Kitendo cha kumkamata mtu kimehusishwa na aina mbalimbali zakanuni za kiutendaji. Kuna wakati ambapo polisi hutumia nguvu nyingi wakati wa kukamata, hata pale ambapo mtuhumiwa anakuwa yupo tayari kwenda kwenye kituo cha polisi bila shuruti. Inaonekana kwamba polisi polisi wamejijengea tabia kwamba hatua ya kwanza katika kushughulika na mtuhumiwa ni kumdharau na kumdhalilisha mbele ya ndugu, jamaa na marafiki zake. Sheria haijaelekeza polisi kufanya kazi katika mazingira hayo.

Hatua ya kwanza ambayo sheria inaelekeza ni kukamatwa kwa mtuhumiwa tu. Mara nyingi pale ambapo mtu, anaambiwa kwamba yupo chini ya ulinzi, anapaswa kukamatwa na kuambiwa sababu za kukamatwa kwake. Ni pale tu ambapo mtuhumiwa hukataa kutii agizo la kukamatwa

ndipo polisi anaruhusiwa kugusa mwili wa mtu au kumfunga pingu. Ikiwa mtuhumiwa atakataa kukamatwa, basi polisi wanaruhusiwa kutumia nguvu ya kawaida kuweza kumkamata mtuhumiwa. Muhimu kujua kwamba mtuhumiwa ana haki ya kufahamishwa kosa ambalo anatuhumiwa kabla ya kukamatwa na polisi.

Wakati polisi wanapomkamata mtu, huondoa haki ya msingi ya mtu huyo kuwa huru. Kwa hiyo, kuna taratibu kadhaa ambazo polisi lazima wazifuate kabla ya kumkamata mtu kisheria ili kuhakikisha haki za binadamu zinazingatiwa.

Kwa mujibu wa Sheria ya Mwenendo wa Makosa ya Jinai ya mwaka 1985, mtu aliyekamatwa ana haki kadhaa za kuzingatiwa. Hivyo, afisa anayemkamata mtuhumiwa anapaswa kuhakikisha kwamba lazima azingatie taratibu zote za kisheria za kumkamata mtuhumiwa.

(a) Ni wakati gani afisa anaweza kumkamata mtu?

Kuna idadi ndogo tu ya mazingira ambayo afisa anaweza kumkamata mtu.

- Afisa mwenyewe aliposhuhudia kitendo cha uhalifu;
- Afisa ana sababu ya kuamini kuwa mtu huyo aliyekamatwa alifanya uhalifu;
- Afisa ana hati ya kukamata iliyotolewa na hakimu.

(b) Utaratibu wa kukamata Mtuhumiwa

Utaratibu juu ya kile ambacho afisa anapaswa kufanya wakati wa kukamata nchini Tanzania umetolewa chini ya Sheria ya Mwenendo wa Makosa ya Jinai, ya mwaka 1985. Kwa ujumla, kukamatwa hutokea wakati mtu anayekamatwa anaamini kuwa hayuko huru kuondoka. Afisa hahitaji kumfunga pingu mtuhumiwa, au kumuweka mtuhumiwa katika gari la polisi ingawa polisi mara nyingi hutumia mbinu hizi kujikinga. Polisi pia wanapaswa kusoma Sheria ya Mwenendo wa Makossa ya Jinai, 1985 wakati wa kukamata.

Hata hivyo, polisi lazima asome mbele ya mtuhumiwa haki zake chini ya Sheria ya Mwenendo wa Makosa ya Jinai, 1985 kabla ya mahojiano, kama ambavyo idara nyingi za polisi husisitiza kwamba Haki za watuhumiwa zisomwe kabla ya kukamata. Kwa njia hii, polisi wanaweza kuanza kumhoji mtuhumiwa mara moja, na pia, taarifa yoyote inayotolewa na mtuhumiwa inaweza kutumika dhidi yao. Hatimaye, ingawa polisi daima humwambia mtuhumiwa kwanini amekamatwa, wanaweza kutokuwa na wajibu wa lazima wa kisheria kufanya hivyo.

Moja ya kanuni inayotumia duniani kote ambayo maafisa wa polisi wote wanapaswa kufuata ni kwamba hawaruhusiwi kutumia nguvu nyingi au kumuadhibu mtuhumiwa kikatili. Hii pia imewekwakwa wazi chini ya Sheria ya Jeshi la Polisi na Huduma Saidizi ya mwaka 1969. Kwa ujumla, maafisa wa polisi wanaruhusiwa kutumia kiasi cha chini cha nguvu zinazohitajika ili kujilinda na kumuweka mtuhumiwa chini ya ulinzi wa polisi. Ndiyo sababu watu wanashauriwa kamwe kutokupinga kukamatwa au kujibizana na polisi. Kadri mtuhumiwa anavyopambana kukataa kukamatwa, nguvu zaidi inahitajika kwa polisi kufanya kazi yao. Ikiwa mtuhumiwa anadhani kukamatwa kwake sio halali kisheria au si sahihi anaweza kupinga kukamatwa kwake baadae kwa msaada wa mwanasheria, na ikiwa ni kweli, anaweza kufungua kesi ya haki ya madai.

(c) Upekuzi

Upekuzi inabidi ufanye kwa mujibu wa sheria na taratibu zilizowekwa, kwakuwa huingilia faragha na uhuru wa mtu kwa mujibu wa na Katiba. Hivyo ni muhimu kupata kibali cha upekuzi kutoka kwa mamlaka husika kabla ya kumkamata mtuhumiwa.

Zipo aina mbili za upekuzi;

- Kwanza ni kibali kutoka katika kituo cha polisi husika. Kibali hiki kinaweza kutolewa kwa mtu yeyote ikiwa ni pamoja na maafisa wa polisi.
- Kibali chaa pili ni kibali cha upekuzi kinachotolewa na mahakama.

7.1.2 Kuwekwa kizuizini

Ikumbukwe kwamba, kuwekwa kizuizini kwa Mtetezi wa Haki za Binadamu au mtu mwingine yeyote kunazuia uhuru wa mtu kwa mujibu wa Katiba ya Jamhuri ya Muungano wa Tanzania. Ndiyo maana kuwekwa kizuizini kwa mtu kuna kikomo cha muda. Kikomo kikubwa cha muda uliopo kisheria ni masaa 24 ambayo mtu aliyekamatwa anatakiwa kupelekwa mahakamani au kupewa dhamana ya polisi.

Endapo Mtetezi wa Haki za Binadamu au mtu mwingine yeyote atakaa chini ya ulinzi wa polisi au sehemu nyingine kizuizini bila ya kupelekwa mahakamani au kupewa dhamana ya polisi, inashauriwa kwamba maombi ya dhamana na / au maombi ya mtuhumiwa kuletwa mahakamani yanapaswa kupelekwa mahakamani ili kuomba amri ya mahakama kwamba mtu huyo aletwe mahakamani ili kukabiliana na mashtaka yanayomkabili. Katika kupeleka maombi haya, Mtetezi wa Haki za Binadamu anahitaji kupata msaada wa mwanasheria ambapo pia Mtanadao wa Watetezi wa Haki za Binadamu unaweza kuingilia kati na kusaidia.

7.1.3 Mashtaka

Ni muhimu kutambua kwamba, moja ya huduma za ulinzi zinazotolewa na Mtandao wa Watetezi wa Haki za Binadamu ni uwakilishi wa mahakamani. Kwa hiyo Watetezi wa Haki za Binadamu wanaokumbana na changamoto za kisheria wanapaswa kutoa taarifa kwa Mtandao wa Watetezi wa Haki za Binadamu kwa msaada zaidi. Hata hivyo, tunasisitiza Mtetezi wa Haki za Binadamu kuelewa mambo kadhaa yanayohusiana na mashtaka kama mkakati binafsi wa kujilinda. Katika sehemu hii Mtetezi wa Haki za Binadamu atadhaniwa kuwa ni mtuhumiwa. Uendendeshaji wa mashitaka kwa kawaida hufanyika kulingana na hatua zifuatazo;

(a) Hati ya mashtaka (mashtaka)

Shitaka ni msingi wa kufungua kesi ya jinai dhidi ya mtuhumiwa. Hii ni hati ambayo inaelezea makosa na vifungu vya sheria ambavyo mtuhumiwa amevunja, pamoja na taarifa zake binafsi. Mwendesha Mashtaka ataandaa mashitaka ikiwa kesi hiyo inasikilizwa na mahakama ndogo au taarifa kama makosa yanaweza kusikilizwa tu na Mahakama Kuu. Haya ni makosa ambayo yanasikilizwa na Mahakama Kuu tu kama vile ndugu wa damu kuwa katika mahusiano ya kimapenzi, mauaji, uchomaji na uasi.

(b) Kukiri au kukataa mashtaka

Hapa mshitakiwa anatakiwa kukiri au kukataa mashtaka aliyosomewa. Mshitakiwa atatakiwa na mahakama kukubali au kukataa mashtaka dhidi yake. Ikiwa mshitakiwa atakiri kuwa ana hatia lazima kukiri kwake kusiwe na utata, pakiwa na utata tu mahakama itasema mshitakiwa hajakiri kuwa ana hatia. Ikiwa mahakama itathibitisha kuwa mtuhumiwa ana hatia, mwendesha mashtaka ataruhusiwa kuendelea na kesi yake. Ikiwa imeahirishwa mshitakiwa atakuwa na nafasi ya kuomba dhamana, ikiwa kosa lake lina dhamana. Ikiwa mshitakiwa amekiri kuwa ana hatia basi utaratibu utarukwa hadi kumuachia huru au kuhukumiwa.

(c) Dhamana ya Mahakama

Mara nyingi ikiwa mtuhumiwa amekiri kuwa na hatia, maombi ya dhamana hayatumiki tena na dhamana haiwezi kutolewa. Baada ya kukiri au kukataa kosa mtu anapelekwa rumande au anaachiwa kwa dhamana. Dhamana ni haki ya kikatiba chini ya Ibara ya13 (6) (b) ya Katiba ya Jamhuri ya Muungano wa Tanzania 1977, ambapo mtu hudhaniwa kuwa hana hatia hadi mahakama itakapothibitisha kwamba mtu huyo ni mkosaji. Kuna makosa yasiyo na dhamana kama vile Uhaini, wizi wa kutumia silaha, unajisi na mauaji chini ya kifungu cha 148 (5) cha Sheria ya Mwenendo wa Makosa ya Jinai. Dhamana ya polisi inaweza kutolewa kabla ya kesi kwenda mahakamani; dhamana ya mahakama hutolewa wakati ambao kesi imeshapelekwa mahakamani.

(d) Usikilizaji wa Awali

Hii ni hatua muhimu ambapo pande zote zinakutana na rasimu kuhusu uhalisia wa maswala wanayokubaliana ili kuharakisha usikilizwaji wa kesi. Pande zote zinapaswa kukutana na kuamua juu ya mambo ambayo hayana mgogoro na mambo haya hayatakiwi kuletwa wakati kesi inaendelea na kila pande haitakiwi kuthibitisha chochote kuhusu masuala hayo kasoro yale mambo tu ambayo yapo kwenye mgogoro.

(e) Hatua ya Usikilizwaji wa Kesi

Huu ndio wakati kesi inapangwa kwa ajili ya kusikilizwa au kutajwa na mwendesha mashtaka anapaswa kuthibitisha mbele ya mahakama kama kuna kesi dhidi ya mshitakiwa au sio laa.

Kesi upande wa Mwendesha Mashtaka

Hii ni hatua ambapo mwendesha mashtaka anapaswa kuwasilisha kesi yake, ambapo mwendesha mashtaka atawaita mashahidi kutoa ushahidi wao na kuwasilisha ushahidi wowote mwingine unaounga mkono kesi yao, kwa ajili ya mahakama kuamua kama kuna kesi ya kujibu au laa. Ni katika hatua hii ambapo shahidi atahojiwa kwa mara ya kwanza kisha kuhojiwa na upande wa utetezi hatimaye kufuatiwa tena na uchunguzi wa upande wa mashtaka. Muhimu; kwa ujumla, wajibu wa kuthibitisha mashtaka upo upande wa mwendesha mashtaka na kiwango cha kuthibitisha ni bila kuacha shaka ya aina yoyote.

(f) Kuwa au kutokuwa na kesi ya kujibu.

Hii ndio hatua ambapo mahakama inapaswa kuamua kama kuna kesi ya kujibu au laa, kwa kuzingatia ushahidi uliotolewa na upande wa mwendesha mashtaka. Ikiwa hakuna kesi ya kujibu mahakama itamuachia huru mshtakiwa, ikiwa kuna kesi ya kujibu mshtakiwa atakuwa na nafasi ya kutoa ushahidi wake.

(g) Kesi ya Upande wa Utetezi

Kimsingi hapa timu ya upande wa utetezi itawasilisha ushahidi wake, shahidi ataongozwa na wakili wa utetezi, pia na upande wa mashitaka na mwisho ataongozwa tena na upande wa utetezi.

(h) Uwasilishaji wa mwisho.

Huu ni muhtasari wa uwasilishaji kamili kutoka kila upande; upande wa utetezi utakuwa wa kwanza kufanya uwasilisho wao wa mwisho kisha kufuatiwa na upande wa mashtaka. Uwasilishaji wa mwisho unaweza kuwa wa mdomo au wa maandishi, hii lazima iwe na ruhusa ya mahakama.

(h) Kumuachia huru au kumpa kifungo mshitakiwa

Hii ni hatua ambapo mahakama itaamua kwa kutegemea uwasilishaji wa mwendesha mashitaka na upande wa utetezi kama mshitakiwa anapatikana na hatia au la. Kwa hivyo mshitakiwa anaweza kupatikana kuwa hana hatia, ikiwa hana hatia, mchezo unaisha, ataachiwa huru, ikiwa amepatikana na hatia hatua nyingine itafuata.

(i) Sababu za kupunguziwa adhabu.

Wakati mshitakiwa anahukumiwa, upande wa utetezi utapewa nafasi ya kuwasilisha hoja ambazo zitapunguza adhabu na upande wa mashitaka utapewa nafasi kuwasilisha hoja ambazo zitaongeza adhabu.

(j) Hukumu

Hili litakuwa jambo la pili kutoka mwisho, mahakama itasoma hukumu ndani ya siku 90 kwa mujibu wa kifungu cha 311 cha Sheria ya Mwenendo wa Makossa ya Jinai. Mfumo wa hukumu umetolewa chini ya kifungu namba 312 cha Sheria ya Mwenendo wa Makosa ya Jinai.

(k) Ufafanuzi Kuhusu Haki ya Kukata Rufaa

Jaji / hakimu lazima aieleze haki ya kukata rufaa kwa upande wowote ambao haujaridhika na hukumu ya mahakama. Zingatia sheria ya siku sitini iliyopo chini ya kifungu cha 225 cha Sheria ya Mwenendo wa Makosa ya Jinai ambacho kinahitaji upelelezi wa jinai kukamilika ndani ya siku 60 tangu siku ya kuanza isipokuwa kwa baadhi ya makosa mengine makubwa ambayo uchunguzi wake unaweza kuwa wa muda mrefu kama uasi.

Sura ya

8

Kuboresha Ulinzi Ofisini na Nyumbani

8.0 Utangulizi

Usalama katika makao makuu ya shirika au ofisi na katika nyumba za wafanyakazi ni muhimu sana kwa kazi ya watetezi wa haki za binadamu. Muongozo huu unaeleza kwa kina kuhusu jinsi usalama wa ofisi au nyumba inavyoweza kuchambuliwa na kuboreshwa.

8.1 Mambo ya jumla kuzingatiwa katika usalama wa ofisi

Malengo ya kuboresha usalama yanaweza kufupishwa kwa kutumia maneno yafuatayo:

- Kuzuia upatikanaji wa taarifa usio idhinishwa. Katika visa vidogo pia ni lazima kulinda ofisi dhidi ya mashambulizi yanayoweza kutokea (dhidi ya mabomu).
- Udhaifu wa ofisi. Huu unaongeza hatari, kulingana na tishio unalokabiliana nalo. Kwa mfano, ikiwa upo katika hatari ya kuibiwa vifaa au taarifa, lazima uondoe udhaifu huo kwa usahihi. Kengele ya usiku itakua na umuhimu mdogo ikiwa hakuna mtu anayekuja na kuangalia kilichotokea. Kwa upande mwingine, ikiwa kuna vurugu mchana, fensi iliyoimara kwenye mlango au kengele haitakuwa muhimu sana. Kwa kifupi, chukua hatua kulingana na vitisho ambavyo unakumbana navyo na namna unavyovishughulikia.
- Udhaifu wa ofisi lazima upimwe kulingana na vitisho unavyoweza kukabiliana navyo. Hata hivyo, ni muhimu kuweka usawa katika kuchukua hatua sahihi za usalama na kutoa hisia kwa watu wa nje kwamba kuna kitu “kimefichwa” au “kulindwa”. Kwa sababu hii inaweza kukuweka katika hatari. Katika usalama wa ofisi mara nyingi unapaswa za kawaida, hatua ambazo ni za dhahiri zaweza kuchukuliwa ikiwa ni lazima.
- Usalama wa ofisi sio mkubwa kuliko sehemu yake dhaifu. Ikiwa mtu anataka kuingia bila wewe kufahamu, hatachagua njia ngumu zaidi ya kuingia ili kufanya hivyo. Kumbuka kuwa njia rahisi ya kuingia ofisini na kujionea kinachoendelea ndani wakati mwingine ni kubisha mlango na kuingia ndani.

8.2 Mahali pa kuweka ofisi

Mambo ya kuzingatia wakati wa kutafuta mahali pa kuweka ofisi ni:

- Majirani; ikiwa jengo linahusishwa na watu fulani au shughuli fulani za zamani;
- Upatikanaji wa usafiri wa umma na binafsi;
- Hatari ya ajali;
- Jinsi gani jengo linafaa kuweka hatua muhimu za usalama, nk.

Ni muhimu kufanya mapitio ni hatua gani za usalama zinazochukuliwa na wengine katika maeneo jirani. Ikiwa zipo nyingi, hii inaweza kuwa ishara ya eneo kuwa sio salama, kwa mfano, kuhusiana na makosa ya kawaida. Pia ni muhimu kuzungumza na watu katika eneo hilo juu ya hali ya usalama wa eneo husika. Kwa hali yoyote, hakikisha hatua za usalama zinaweza kuchukuliwa bila kuvutia hisia zisizofaa za watu. Pia ni muhimu kujua watu jirani sababu wanaweza kukupatiaa habari kuhusu tuhuma yoyote inayoendelea kwa jirani.

Pia ni muhimu kuangalia ni nani aliyekupangisha. Je, sifa zao ni zipi? Je, wanaweza kuwa na shinikizo kutoka kwa wenye mamlaka? Je! Watakuwa na amani na wewe kuweka hatua za usalama?

Uchaguzi wa ofisi lazima uzingatie nani ambaye anahitaji kuja ofisini. Ofisi ambayo waathirika wanakuja kutafuta ushauri wa kisheria itakuwa na mahitaji tofauti na ofisi ambayo ni maalumu kwa wafanyakazi pekee. Ni muhimu kuzingatia jinsi ambavyo ni rahisi kufikia usafiri wa umma, itakuwa na safari iliyo salama kati ya eneo ambako wafanyakazi wanaishi, ambapo kazi nyingi hufanyika, nk. Maeneo ya jirani yanapaswa kufanyiwa tathmini, hasa ili kuepuka kusafiri katika maeneo ambayo sio salama.

Mara tu eneo likishachaguliwa, ni muhimu kufanya tathmini za mara kwa mara za eneo ambalo linaweza kutofautiana, kwa mfano, kama ‘kipengele kisichohitajika’ kinaingia kwa jirani.

Orodha ya mambo muhimu kuzingatia unapochagua eneo la kuweka Ofisi

UJIRANI:	Takwimu za uhalifu; ukaribu na maeneo yaliyolengwa kwa mashambulizi ya silaha, kama vile mitambo ya kijeshi au serikali; kuhakikisha usalama maeneo ya kujihifadhi; mashirika mengine ya kitaifa au ya kimataifa ambayo una uhusiano nayo.
MAHUSIANO:	Aina ya watu katika ujirani; mmiliki / mpangishaji, wapangaji wa zamani; matumizi ya zamani ya jengo hilo.
UPATIKANAJI:	Njia moja au njia nyingi nzuri za usafiri (nyingi zaidi, ni bora zaidi); upatikanaji wa usafiri wa umma na binafsi.
HUDUMA ZA MSINGI:	Maji, umeme na simu
MWANGA KATIKA MTAA:	Katika eneo jirani
VIASHIRIA VYA AJALI AU HATARI ZA ASILI:	Moto, mafuriko mazito, maporomoko ya ardhi, kutupa vifaa vya hatari, viwanda vilivyo na michakato inayosababisha madhara, nk.

MUUNDO WA NJE:	Uimara wa miundo, kituo kwa ajili ya kufunga vifaa vya usalama, milango na madirisha, mzunguko na vikwazo vya ulinzi, pointi za kufikia (tazama hapa chini).
VYOMBO VYA MOTO VYA USAFIRI:	Karakana au angalau maegesho ya magari

7.3 Mambo mengine muhimu ya kuzingatia kuboresha usalama nyumbani na ofisini;

(a) Uzio ikiwa ni pamoja na uzio wa umeme. Ni muhimu kwamba ambapo rasilimali inaruhusu, ofisi za Watetezi wa Haki za Binadamu zinapaswa kuwa na uzio na pale inapowezekana, zinapaswa kuwa na uzio wa umeme.

(b) Vifaa vya ofisi na mafunzo (sanduku la huduma ya kwanza, zima moto mafunzo ya mara kwa mara ya namna ya kuzitumia. Tumia pia namba za milio ya bure.

(c) Funguo za Ofisi hazipaswi kuwa sehemu ya wazi hasa kwa wageni. Zinapaswa kuwa sehem ambapo watu wachache wanaweza kuziona. Fanya mabadiliko ya mara kwa mara ya neon la siri kwa usalama.

(d) Ukiwa unatoka ofisini kwako, hata ikiwa ni kwa dakika chache, hakikisha unafunga kompyuta yako na kulinda hati zako za siri ili watoto na wavamizi wasizifikie kwa urahisi. siojiunga wawe rahisi kufikia. Hakikisha kwamba milango ya ofisi na baraza imefungwa, iwe upo ndani au nje ya ofisi. Kabla ya kuondoka ofisini kwako kila siku, hakikisha unasafisha dawati lako na uondoe hati yoyote. Pia, hakikisha unafunga madirisha yako, kabati za faili na dawati.

(e) Wekea alama Vifaa vya Ofisi yako. Hakikisha unawekea alama vifaa vya ofisi yako na alama za kitambulisho (ID), mihuri au stika na idadi yako ya hesabu na nembo.

(f) Weka orodha kamili ya vitu vyote katika ofisi yako, mahali panapoonekana (hasa kwenye ukuta wa ofisi), ili wewe na wafanyakazi wako waweza kuhakikisha wakati wowote kwamba kila kitu kiko katika mahali pake.

(g) Vaa beji za kitambulisho. Hakikisha wafanyakazi wako wote wana majina yao yameandikwa kwenye beji zao za utambulisho. Zaidi, wateja wa ofisi wanapaswa kupewa beji za utambulisho wa wageni. Hii ni kipimo kikubwa cha usalama ambacho unaweza kutumia kwa faida yako. Kwa hiyo, unaweza kujua nani anayekuja au kwenda nje ya eneo lako la ofisi.

(h) Sakinisha mifumo ya CCTV. Faida za mifumo ya CCTV ni nyingi. Inatumika kama mwongozo kwa wafanyakazi wako na pia njia ya kukamata wahusika au wahalifu katika ofisi yako. Kufunga mifumo ya CCTV ni mojawapo ya njia rahisi zaidi na za ubunifu za kuongeza usalama katika ofisi yako. Ikiwa unataka kuimarisha usalama wa ofisi yako au mahali pa kazi, hakikisha unaweka CCTV katika karakana na mlango wa kuingia katika ofisi yako.

(i) Wekeza katika mifumo ya miito ya sauti. Njia bora zaidi ya kuimarisha usalama wa ofisi yako ni kwa kuongeza mifumo ya miito ya sauti. Faida ni sawa na ufungaji wa kamera za CCTV mahali pa kazi. Kufunga mifumo ya miito ya sauti itafanya kazi kama kizuizi, mara tu watu wakiona eneo linalindwa na silaha ya miito ya sauti, watakuwa makini jinsi wanavyoingia na kwenda nje ya mahali hapo. Uzuri wa mifumo ya miito ya sauti ni kwamba itaonya mamlaka kama kuna kiashiria chochote cha shughuli za uhalifu, na wavamizi au wezi wataepuka kuja ofisini kwako.

(j) Weka Nywila zako Binafsi. Hakikisha beji zako za utambulisho, funguo, nywila za kompyuta, na kadi za muhimu ni zipo sehem salama. Unaweza kufanya hivyo kwa kuhakikisha humpi mtu ambaye huwezi kumwamini. Ikiwa inawezekana kwako, hakikisha usiitoe mara ya kwanza. Kuna watu ambao utawapa kwa uaminifu, na watatumia upendeleo huo vibaya,

(k) Jua ujirani wako. Unajua majirani zako na ujirani wako? Wahalifu mara nyingi zaidi kabla ya kuamua wapi na wakati gani wa kuingia na kufanya uhalifu, huangalia wakati gani wewe na familia yako huwa mnakuja na kuondoka. Kujua jirani yako na watu wanaoishi karibu na wewe itasaidia kuona wanaohusika au kutiliwa mashaka. Majirani zako wanaweza kuwa mstari wa kwanza wa ulinzi dhidi ya uvamizi nyumbani kwako wakati usipokuwepo. Wanajua eneo hilo na wanaweza kusaidia kutazama nyumbani kwako wakati uko mbali - lakini hawawezi kufanya hivyo ikiwa hawajui. Fanya jitihada za kukutana na majirani zako wapya na kuunda mahusiano mazuri ili uwe na watu wa kutegemea. Ikiwa kitu kibaya kinatokea katika eneo lako, jirani mwema atakufahamisha au kukujulisha. Kuzungumza na majirani zako kuhusu watu wanaotiliwa mashaka au magari yanayohusika.

(l) Mjue mpangishaji wako. Ikiwa mpangishaji atakubaliana na wewe kuweka vifaa vya usalama katika ofisi yako

(m) Weka mwanga juu ya maeneo yote yanayozunguka ofisi na nyumba yako.

Sura ya

9

Usalama Katika Mawasiliano na Teknolojia ya Habari

9.0 Utangulizi:

Wewe ni Mtetezi wa Haki za Binadamu wa Kiafrika wa karne ya 21. Una silaha ya akili yako, hisia kali ya haki katika jamii, uhusiano na jamii za ndani, simu ya mkononi, skanu (iPad) na kompyuta mpakato. Miaka ishirini iliyopita vitu vitatu vya mwanzo vilikuwepo lakini simu ya mkononi na kompyuta mpakato ni vigeni katika karne ya 21. Teknolojia ya digitali inafanya uwezo wetu wa kutathmini hatari yetu ya kibinafsi na ya kitaaluma kuwa mgumu kwa sababu zinakuwa hazieleweki kwa urahisi. Bila ujuzi wa kitaaluma na kiufundi ni vigumu kutambua inapotokea vifaa hivyo vinavyohifadhi nyaraka nyeti vinapoziachia taarifa hizo kwa watu wengine. Pamoja na Sheria ya Makosa ya Mtandao, 2015, Kanuni za Maudhui Mtandaoni 2018 (The Online Contents Regulations, 2018) ambayo kwa kiasi kikubwa ina vikwazo dhidi ya matumizi ya majukwaa ya mtandaoni kama barua pepe, Skype, Facebook Messenger, Instagram, Twitter, Whatsapp, youtube na kadhalika, ni muhimu kuwa salama unapokuwa mitandaoni.

9.1 Kuzungumza

Sio lazima taarifa ipitie kwenye mitandao ndipo itakapoweza kuchukuliwa na mtu mwingine kinyume cha sheria. Wakati wa kujadili masuala nyeti, fikiria mambo yafuatayo:

- Unawaamini watu unaozungumza nao?
- Je! Wanahitaji kujua taarifa unazowapa?
- Je! Uko katika mazingira salama? Vifaa vya kunasa mazungumzo au vifaa vingine vya kusikiliza mara nyingi hasa hupandikizwa katika maeneo ambapo watu hudhani kuwa ni salama, kama ofisi za faragha, mitaa yenye watu wengi, vitanda vya nyumbani na kwenye magari.

Inaweza kuwa vigumu kujua jibu la swali la tatu, kwa sababu vipaza sauti au vifaa vya kunasa sauti vinaweza kupandikizwa katika chumba kurekodi au kupeleka kila kitu kinachosema huko. Vinasa sauti pia vinavyotoa mwanga vinaweza kuelekezwa kwenye madirisha kutoka umbali mkubwa ili kusikiliza kile kinachosemwa ndani ya jengo. Mapazia mazito hutoa ulinzi dhidi ya vinasa sauti vinavyotoa mwanga (laser bugs), kama vile kufunga madirisha mara mbili na vioo. Baadhi ya majengo salama yana seti mbili za madirisha zilizowekwa katika ofisi ili kupunguza hatari ya vifaa vya kunasa sauti vinavyotoa mwanga.

(a) Unaweza kufanya nini?

- Daima dhania kuwa kuna mtu anasikiliza ndani. Kwa mtazamo huo wa kuwa na hofu kiasi kidogo, unakua na uwezekano mkubwa wa kuwa makini wakati unapokuwa na masuala ya siri.

- Wataalamu maalum wa vinasa sauti wanaweza kutumika kuchunguza na kugundua vinasa sauti, lakini inaweza kuwa ni vigumu kuwapata. Pia, wakati mwingine wataalamu hao wanaweza wakawa wamehusika katika kuweka vinasa sauti vya awali. Wakati wa kuondoa vinasa sauti, wanaweza kufanikiwa kupata vifaa vichache na "vidogo" tu au si ajabu wakakosa chochote na kutangaza ofisi ziko safi".
- Wafanyakazi wote wa usafi wa ofisi wanaweza kuwa tishio kubwa la usalama. Wao huingia mara kwa mara katika ofisi yako na kusafisha pamoja na kuchukua uchafu wote kila siku. Wafanyakazi wote wanapaswa kuchunguzwa kwa makini kwa usalama na hii inapaswa kuwa muendelezo, kwani wafanyakazi wanaweza kuathiriwa baada ya kujiunga na shirika lako.
- Badilisha vyumba vya mikutano mara nyingi iwezekanavyo. Kadiri vyumba na maeneo ya mikutano unayotumia kujadili na kubadilishana habari yanapokua mengi, ndivyo rasilimali watu na vifaa zaidi vitatakiwa kutumiwa kusikiliza na kupata taarifa kutoka kwako.
- Jihadhari na zawadi zinazoletwa kwaajili yako, hasa zawadi zinazolengwa kukaa kwa muda mrefu kama vile kalamu ya gharama kubwa, beji, au zinazotumika katika ofisi yako, kama karatasi nzuri au picha kubwa. Aina hizi za vitu zimetumiwa katika siku za nyuma kusikiliza mazungumzo ya faragha ya watu.
- Fikiria kuwa sehemu fulani ya taarifa yako imeathiriwa wakati wowote. Unaweza kubadilisha mipango na lugha mara kwa mara, na kuwapa wasikilizaji wako vipande vipande tu vya habari halisi. Wakati mwingine jaribu kutoa maelezo ya uongo ili uone ikiwa kuna mtu yeyote anatumia au anaitikia.
- Kupunguza ufanisi wa kinasa sauti kinachotumia mwanga, jadili maswala nyeti ukiwa kwenye chumba cha chini au chumba kisicho na madirisha. Vifaa vingine vya kunasa sauti vinavyotumia mwanga vinaweza kushindwa kufanya kazi vizuri wakati wa mvua na mabadiliko mengine ya anga.
- Cheza sauti iliyorekodiwa bila kelele au wimbo maarufu kuingiliana na vifaa vya kunasa sauti. Teknolojia ya gharama kubwa tu inaweza kuchuja kelele ili kusikia mazungumzo.
- Maeneo mengi mapana yanaweza kuwa na manufaa na yenye madhara. Kufanya mkutano katika mahali ampapo watu wengi hawafiki hufanya iwe rahisi kuona ikiwa unafuatiliwa au unatazamwa, lakini inakuwa vigumu kuepuka kwa kuingia ndani. Makundi ya watu hufanya iwe rahisi kuunganisha, lakini ni ngumu sana kuonekana na kusikiwa.

(b) Simu za mkononi

Simu zote zinaweza kusikilizwa ikiwa msikilizaji ana uwezo wa kutosha wa teknolojia. Hakuna simu inayoweza kudhaniwa kuwa salama. Simu za mkononi za analojia si salama zaidi kuliko simu za mkononi za dijitali, na zote mbili sio salama zaidi kuliko simu za mezani.

Sehemu uliyopo na mazungumzo yako yanaweza kunaswa kupitia ufuatiliaji wa simu. Si lazima uwe unaongea na simu ili kufuatiliwa - hii inaweza kufanyika wakati wowote simu yako ya mkononi inapokua imewashwa.

Usihifadhi habari kama majina nyeti na namba kwenye kumbukumbu ya simu yako. Ikiwa simu yako imeibiwa, taarifa hizi zinaweza kutumika kufuatilia baadae na kuathiri watu unaotaka kuwalinda.

(c) Mambo ya msingi kuzingatia katika usalama wa kompyuta na faili

- Fungia kompyuta yako wakati wa kuondoka ofisini, kama inawezekana. Zima kompyuta yako unzpotoka.
- Tumia vifaa vya kuzuia kuongezeka kwa umeme (kupungua na kuongezeka kwa umeme kunaweza kuharibu kompyuta yako).
- Weka kitunza kumbukumbu, ikiwa ni pamoja na faili za karatasi, katika mahali salama na tofauti na mahali pa kawaida. Hakikisha vitunza kumbukumbu viko salama kwa kuviwekea nywila au kuviweka kwenye kompyuta inayolindwa na nywila za kisasa.
- Kupunguza hatari ya mtu kuingia kwenye kompyuta yako, linda kompyuta yako na mara zote zima kompyuta yako wakati wa kuondoka.
- Weka nywila kwenye faili zako ikiwa mtu anaweza kufikia kompyuta yako au pitia tena kuhakikisha ulinzi wako. Ikiwa kompyuta yako imeibiwa au kuharibiwa, utakuwa na uwezo wa kurejesha faili zako ikiwa umeweka ulinzi katika vitunza kumbukumbu (secure back-up) kila siku. Tunza nywila zako mbali na ofisi yako katika mahali salama. Faili zilizofutika haziwezi kurudishwa upya ikiwa umezifuta kwa kutumia kifutio cha PGP au huduma nyingine, badala ya kuziweka kwenye file la takataka la kompyuta (Recycle been).
- Kompyuta yako inaweza kupangiliwa katika hali itakayoifanya itume taarifa au faili zako kwa mtu mwingine na kukuweka katika hatari bila wewe kujua. Ili kuepuka hili, nunua kompyuta yako kutoka kwenye chanzo cha kuaminika, futa kila kitu kwenye kompyuta unapoinunua na kuanza kuitumia kwa mara ya kwanza, na kisha weka programu unayotaka. Tumia mafundi wa kuaminika kutoa huduma kwenye kompyuta yako na kuwaangalia wakati wote.
- Zingatia kuondoa uhusiano wa simu na kompyuta yako / modem, au vinginevyo zima muunganiko wa intaneti, unapoondoka kwenye kompyuta yako. Kwa njia hii, programu

zinazoletwa kwenye computer yako ili kukudhuru katikati ya usiku hazitafanya kazi. Usiache kompyuta yako ikiwa inawaka wakati unapoondoka. Jaribu kuweka programu ambayo italemaza au kuzuia upatikanaji wa taarifa katika kompyuta yako baada ya muda fulani inapokaa bila kutumiwa. Kwa njia hii, kompyuta yako haitakuwa hatarini wakati unapopata kahawa au kutoa nakala unapokua ofisini.

- Katika matumizi yako ya wavuti, fungua faili jipya ili uweze kujua ni aina gani ya faili kabla ya kulifungua. Hutakiwi kufungua virusi kwa kufungua faili ambayo ulifikiri ilikuwa faili ya maandishi. Katika Internet Explorer, nenda kwenye orodha ya vifaa (Tools) na chagua Chaguo za folda. Bonyeza "Angalia" (View) na uhakikishe kuwa sanduku la kuficha taarifa za nyongeza kwa taarifa zinazotambulika hazijaangaliwa.

(d) Mambo ya msingi kuzingatiwa katika Usalama wa Mtandao

Virusi na matatizo mengine, kama vile program zenye virusi, zinaweza kutoka popote; hata marafiki wanaweza kueneza virusi bila kujua. Tumia programu nzuri za kupambana na virusi (anti-virus) na uendelee kuziweka kumbukumbu mpya mara kwa mara ili ziweze kujiendesha zenyewe mtandaoni. Virusi wapya wanaundwa mara kwa mara na kugunduliwa, kwa hiyo angalia Maktaba ya Habari ya Virusi kwenye www.vil.nai.com kwa taarifa za virusi vya hivi karibuni na namna ya kujilinda navyo.

Virusi huenea kwa njia ya barua pepe, kwa hivyo fanya mawasiliano kwa barua pepe salama (angalia hapa chini). Virusi ni programu moja iliyoundwa ili kujizalisha na kuongezeka, inaweza iwe au isiwe mbaya. Programu zenye virusi kama "Trojans" zimeundwa kumfanya mtu wa tatu (au mtu yeyote!) aweze kuifikia kompyuta yako bila wewe kujua.

Anwani ya barua pepe inaweza kufungwa au kutumiwa na mtu mwingine mbali na mmiliki halali wa anuani hiyo. Hii inaweza kufanywa kwa kuingia katika kompyuta na nywila ya mtu mwingine, kwa kuvamia na kuiba, au kwa kutumia anwani inayoonekana kuwa anwani ya mmiliki husika. Kwa mfano, kwa kubadilisha helufi "l" na namba "1", unaweza kuunda anwani sawa na watu wengi hawatagundua tofauti.

Ili kuepuka kudanganywa, tumia mistari yenye maana na mara kwa mara uulize maswali ambayo mtu husika pekee ndiye atakayeweza kujibu;

- Hakikisha maombi yoyote ya taarifa unayoyatilia shaka unayafuatilia kwa njia nyingine ya mawasiliano.
- Weka shughuli zako unapopitia mtandao binafsi kwa kutokukubali kujirudia na kwa kufuta wavuti yako baada ya kila unapomaliza kutumia mtandao. Katika Internet Explorer, nenda kwenye 'Vifaa' (Tools), kisha 'Machaguo' (Options). Katika Netscape Navigator, nenda kwenye Hariri, kisha Mapendeleo. Wakati upo katika mojawapo ya sehemu hizi, futa historia yako yote uliyotumia katika mtandao. Kumbuka kufuta alama zako zote pia. Watazamaji pia

wanaweka kumbukumbu za tovuti unazozitembelea kwenye faili la taarifa zilizotembelewa, hivyo tafuta mafaili ambayo yanapaswa kufutwa kwenye mfumo wako.

- Boresha wavuti ili kuweka taarifa zako katika faili zenye nywila ili mtu asiyehusika asiweze kuziona. Hii itasaidia kulinda maelezo yoyote unayotaka kupitisha salama juu ya wavuti, ikiwa ni pamoja na nywila na data zingine nyeti zilizowasilishwa katika fomu. Weka programu ili kuboresha usalama wa program zote zilizotumiwa, hasa Microsoft Office, Microsoft Internet Explorer na Netscape.
- Usitumie kompyuta inayotumika kuhifadhi taarifa nyeti katika kupitia taarifa zisizo muhimu kwenye mtandao.

(e) Mambo ya muhimu kuzingatia katika usalama wa Barua Pepe

Haya ni mambo muhimu katika usalama wa barua pepe ambayo wewe na marafiki zako wote na washirika wako lazima mfuate ili kujihakikishia usalama wenu. Wajulishe kuwa hutafungua barua pepe zao isipokuwa kama watatuma taratibu za kiusalama.

- Usifungue barua pepe kutoka kwa mtu usiyemjua.
- Usiendelee kutuma kwa watu wengine barua pepe iliyotoka kwa mtu usiyemjua, au ambayo imetoka kwa mtu ambaye humjui. Barua pepe zote za “kuwa na mawazo ya furaha” ambazo watu hutumiana zinaweza kuwa na virusi. Kwa kuwatumia marafiki na washirika wako unaweza kuwa unawaambukiza virusi kwenye kompyuta zao. Ikiwa umeupenda ujumbe, uandike na ujitumie mwenyewe. Ikiwa kuuandika upya haina thamani ya muda wako, labda si ujumbe muhimu.
- Usipakue au kufungua kiambatisho isipokuwa unajua kinahusiana na nini na ambacho ni salama. Zima chaguzi za kupakua moja kwa moja katika programu yako ya barua pepe. Virusi vingi na programu huenea vyenyewe kama “minyoo” na vidudu vya kisasa mara nyingi huonekana kuletwa na mtu unayemjua. Vidudu vidogo vinachunguza kitabu chako cha anwani, hasa ikiwa unatumia Microsoft Outlook au Outlook Express, na ukaiga kwa kukijenga kama kiambatanisho muhimu kutoka kwa washirika halali. Saini barua pepe zako zote kwa kutumia programu ya PGP, hii inaweza kupunguza mchanganyiko zaidi wa virusi katika viambatanisho vyisivyo na virusi ambavyo unatuma kwa wenzako (PGP ni programu ya kuhifadhi taarifa, tafadhali angalia hapa chini)
- Usitumie lugha ya programu/viunganishi vya mtandaoni (HTML and MIME) katika barua pepe yako – tumia ujumbe wa kawaida. Barua pepe zenye viunganishi vya mtandaoni zinaweza kuwa na programu hatari zinazoweza huingilia na kuharibu faili zako za kompyuta.
- Ikiwa unatumia programu ya Outlook au Outlook Express, funga chaguzi za mapitio ya skrini (Preview screen options).

- Weka nywila kwenye barua pepe yako wakati wowote iwezekanavyo. Barua pepe ambayo haina nywila ni kama kadi ya posta ambayo inaweza kusomwa na mtu yeyote anayeiona au anayeipata. Barua pepe iliyofichwa ni kama barua katika bahasha ambayo ni salama.
- Tumia kichwa cha ujumbe chenye maana ili msomaji ajue kwamba ulilenga kutuma ujumbe. Waambie marafiki zako na wafanyakazi wenzako daima waandike kitu fulani katika kichwa cha ujumbe ili ujue kwamba ni kweli wao ndio waliotuma ujumbe. Vinginevyo mtu mwingine anaweza kuingilia mawasiliano yenu, au visusi aina ya 'Trojan' inaweza kutuma programu iliyo ambukizwa katika orodha yako yote ya barua pepe, ikiwa ni pamoja na wewe mwenyewe. Hata hivyo, usitumie vichwa vya ujumbe vinavyotoa taarifa inayotakiwa kuwa salama katika barua pepe zilizofichwa. Kumbuka, kichwa cha ujumbe hakifichwi kwa nywila na unaweza kutoa asili ya taarifa zilizohifadhiwa, ambayo inaweza kusababisha mashambulizi. Programu nyingi zinazotumika kuvamia mtandaoni siku hizi zinanakili moja kwa moja vichwa vya kuvutia vya barua pepe kama vile "ripoti", "siri" "binafsi" na vichwa vingine vinavyoonyesha kuwa ujumbe ni wa manufaa/muhimu.
- Kamwe usitume barua pepe kwenye kikundi kikubwa kilichoorodheshwa kwenye "To" au "CC". Badala yake, tuma ujumbe kwako mwenyewe na ujumuishe jina la kila mtu katika mistari "bcc". Hii ni njia bora na ya kawaida ya kutunza faragha.
- Kamwe usijibu barua pepe zilizokwenye faili la spam, hata kuomba kuondolewa kwenye orodha. Spam hutuma barua pepe kwenye orodha ya barua pepe nyingi zilizojificha na hazijulikani ni zipi zinazotumika- inamaanisha kuwa mtu anatumia anwani ya barua pepe kikamilifu. Kwa kujibu, seva inakutambua kama uko "hai" na utakuwa na uwezekano wa kupokea spam nyingi zaidi.
- Ikiwezekana, tunza kompyuta tofauti, usiounganishwa na nyingine yoyote, ambayo inakubali barua pepe za jumla na haina faili za data.

(f) Vidokezo vya jumla kwa watoa huduma za internet na zaidi

Barua pepe zilizotumwa bila maandishi au zisizojulikana kwenye mtandao zinaweza kusomwa na watu wengi zaidi, ikiwa wakifanya jitihada za namna hiyo. Mojawapo ya haya inaweza kuwa Mtoa huduma wa Internet wa ndani (ISP) au ISP yoyote ambaye barua pepe zako zinapita. Barua pepe inasafiri kupitia kompyuta nyingi ili kutoka kwa mtumaji kwenda kwa mpokeaji; inapita mipaka ya kijiografia na inaweza kupita kwenye seva za nchi nyingine hata kama unatuma barua pepe ndani ya nchi moja.

Baadhi ya vidokezo vya jumla juu ya masuala ya kawaida ambayo hayaeleweki kwa watumiaji wa internet:

- Nywila-inayolinda faili inatoa mchango mdogo sana kulinda faili ambayo haifai kufanya kwa nyaraka zenye taarifa nyeti. Inatoa tu maana ndogo ya usalama.

- Kufunga faili haizuii mtu kuangalia kilichopo ndani ya faili.
- Ikiwa unataka kuthibitisha faili au barua pepe imetumwa kiusalama, tumia programu maalumu ili kuruhusu wahusika tu kuona taarifa hizo (angalia www privaterra.com).
- Ikiwa unataka kutuma barua pepe au hati kwa usalama, tumia njia ya kuifunga kuanzia mwanzo hadi itakapofika kwa mpokeaji wa mwisho. Haifai kutuma barua pepe iliyofungwa kutoka ofisi ya kazi hadi New York au London au mahali pengine na kisha kuruhusu barua pepe hiyo itumwe bila kufichwa/kufungwa kwenda kwa mtu mwingine.
- Mtandao ni wa kidunia kiasili. Hakuna tofauti kati ya kutuma barua pepe kati ya ofisi mbili huko Manhattan na kutuma barua pepe kutoka kwenye café ya internet huko Afrika Kusini hadi kwenye kompyuta ya ofisi ya London.
- Tumia programu ambayo watu husika tu wanaweza kufikia data kwenye kompyuta (encryption), hata kama barua pepe au data unayotuma sio nyeti!
- Hakikisha kompyuta unayoyotumia ina programu ya ulinzi wa virusi. Virusi vingi vimeandikwa ili kuchukua taarifa kutoka kwenye kompyuta yako, ikiwa ni maudhui yako au faili zako za barua pepe, ikiwa ni pamoja na vitabu vya barua pepe.
- Hakikisha programu yako imeidhinishwa vizuri. Ikiwa unatumia programu ambazo hazijaizinishwa, unakuwa mdukuzi wa programu badala ya kuwa mwanaharakati wa haki za binadamu machoni mwa serikali na vyombo vya habari. Chaguo bora ni kutumia programu ya chanzo wazi - ni bure!
- Hakuna suluhisho la usalama wa asilimia mia moja ikiwa unatumia mtandao. Jihadhari kwamba mtu anaweza “kudukua kijamii” katika mfumo kwa kujifanya kuwa mtu asiyekuwa kwenye simu au kwa barua pepe. Tumia uelewa wako mwenyewe na akili ya kawaida.

(g) Mambo mengine muhimu:

- Daima hifadhi barua pepe zako katika fomu iliyofichwa (encrypted). Unaweza daima kuifichua (decrypt) tena baadaye, lakini ikiwa mtu anayo kompyuta yako, ni hatari zaidi kama haijawahi kufichwa.
- Uendelee na kila mtu ambaye mnatumiana barua pepe zilizofichwa ili uhakikishe kuwa hawafichui na kupeleka barua pepe, au kujibu bila kujisumbua kuzificha. Uvivu binafsi ni tishio kubwa katika mawasiliano yako.
- Huenda ungependa kuunda akaunti za barua pepe salama kwa watu wanaojifunza kwa vitendo, ambazo hazitumiwi kwa kawaida na hivyo hazichukuliwi na seva za spam. Anwani hizi zinapaswa kuchunguzwa mara kwa mara lakini hazitumiwi, ila kwa wafanyakazi wanaojifunza kwa vitendo. Kwa njia hii unaweza kuharibu anwani za barua pepe ambazo zinapata spam nyingi bila kuhatarisha msingi wako wa mawasiliano.

(h) Internet na sheria

Kufuatia kutungwa kwa Sheria ya Makosa ya Mtandao, 2015, Kanuni za Maudhui ya Mtandao, 2018 na Sheria ya Huduma za Vyombo vya habari, 2016, mawasiliano yamezuiliwa kwa kiwango kikubwa sana. Kwa hiyo ni muhimu kwa mtetezi wa haki za binadamu kuhakikisha;

- Kamwe husambazi na / au kutuma ujumbe kwenye vyombo vya habari vyovyote vya kijamii ambavyo hauna uhakika wa uhalali wake. Sheria ya Makosa ya Mtandao, 2015 ipo daima kukunasa mara moja unapoikiuka.
- Weka mawasiliano yako salama. Unaweza kupakua programu ya bure inayojulikana kama Automatic Call Reccorder moja kwa moja kwenye simu ili kurecodi mawasiliano yako yote na kukusaidia katika marejeo ya baadaye.
- Epuka kusambaza video za ngono au picha nyingine yoyote ya ngono
- Epuka kutumia lugha ya matusi kwenye vyombo vya habari vya kijamii
- Hupaswi kuendesha jukwaa lolote la mtandaoni ambalo linatakiwa kusajiliwa lakini haujasajili.

KUMBUKA: Yaliyopo hapo juu sio orodha kamili ya kile ambacho haupaswi kufanya, watetezi wa haki za binadamu wanahimizwa kutafuta muda na kupitia sheria zilizoelezwa hapo juu kwa ajili ya marejeo yao na kuongeza ufahamu.

Sura ya

10 Kutathmini Utendaji wa Usalama wa Shirika

10.0 Utangulizi

Kama shirika, kuna uwezekano kwamba tayari kuna hatua za usalama zilizopo. Wakati huo huo labda huhisi kama kuna nafasi ya kuboresha – kawaida ni Kujua ni wapi pakuanzia. Inaweza kuonekana kuwa kubwa sana kwa hivyo ni wazo nzuri kufanya tathmini ili kupata maelezo ya kweli ya usalama wa shirika uliloanzisha.

Kuna watu muhimu ambao wanapaswa kuingizwa katika mchakato huu. Hizi zinaweza kutofautiana shirika na shirika na inaweza kuwa na manufaa kuingiza washauri wa nje ili kusaidia kuongoza mchakato pia. Kwa mfano:

Ndani - Bodi ya wakurugenzi, mkurugenzi mtendaji, wafanyakazi wa ngazi za juu, wafanyakazi wa kawaida na wakujitolea.

Nje - Waajiri, washauri wa nje na wakufunzi

Kuhusisha kila mmoja wa watendaji hawa kuna manufaa na hasara na ni muhimu kwamba mchakato unafanywa kwa njia ya umoja, shirikishi, uwazi na isiyo ya kuhukumu. Mpangilio rasmi ndani ya mashirika unahitaji kubaki nyeti kwa mahitaji ya programu yao na wafanyakazi wanaojifunza kwa vitendo au wakujitolea ambao wanaweza kukabiliwa na hatari kubwa katika kazi zao za siku hadi siku. Wafanyakazi na wanaojitolea wanapaswa pia kuheshimu ukweli kwamba usimamizi unakabiliwa na kazi ngumu katika kusimamia njia ya usalama.

10.1 Vigezo vya tathmini

Tunaweza kuanza kwa kuangalia masuala na viashiria vyenye uhalisia ili kusaidia kuchunguza jinsi taratibu za usalama zinazingatiwa na wafanyakazi. Zingatia pointi zifuatazo:

- Uzoefu wa usalama uliopatikana: Je, wafanyakazi wana uzoefu wa kutekeleza utendaji wa usalama? Je! Uzoefu huu umeenea sawasawa kwa wafanyakazi, au kujilimbikizia kati ya watu wachache?
- Mafunzo ya usalama. Mafunzo ya Usalama kupitia kozi au kupitia mpango wa watu binafsi wakati wa kazi za kila siku. Rasilimali, muda na nafasi zinahitajika kupatikana kwa mafunzo (ama rasmi au yasiyo rasmi). Je, mafunzo hayo yanapatikana kwa wanachama wa shirika? Je hii inajumuisha mafunzo juu ya ustawi wa kisaikolojia na kijamii na usalama wa kidijitali?

- Mtazamo na ufahamu: Je, watu wanafahamu umuhimu wa usalama na ulinzi? Je! Mtazamo wao juu yake ni chanya na wazi kufanyiwa maboresho? Je! Wanajua vikwazo gani wanavyokumbana navyo? Je, mtazamo na uelewa kuhusu usalama wa dijitali, usalama wa nje na ustawi wa kisaikolojia wa jamii unagawanywa katika shirika?
- Mpango wa Usalama: Mpango wa usalama unahusiana na kazi zinazofanywa? Ni mara ngapi uchambuzi wa mazingira umefanywa na mpango ya usalama umeundwa? Je! Mipango inapitiwa mara kwa mara, na inajumuisha usimamizi wa vifaa vya dijitali?
- Mgawanyo wa kazi na majukumu: Je, Kuna mgawanyo wa wazi wa majukumu ya utekelezaji wa mpango wa usalama wetu? Je, majukumu haya yamezingatiwa kwa kiasi gani, na ni vipi vikwazo vinavyoonekana?
- Umiliki na kufuata sheria: Watu wanahusikaje katika mpango wa usalama wa shirika, na kwa kiwango gani wanazingatia mipango iliyopo? Je, ni matatizo gani yanayotokea hapa, na yanaweza kusuluhishwa? Je Mchakato unaweza kufanywa shirikishi zaidi?
- Majibu ya matukio ya usalama: Ni mara ngapi matukio ya usalama yanagawanywa kwa watu? Ni mara ngapi yanachambuliwa na hatimaye kufanyiwa kazi ikiwa kunaulazima?
- Tathmini ya mara kwa mara: Mikakati na mipango ya usalama hupangwa mara ngapi? Je, kuna mchakato mahususi kwa ajili ya hili, au in ategemea na mazingira? Inawezekana kufanywa mara kwa mara au zaidi? Je matatizo gani yanayojitokeza na yanawezaje kutatuliwa?

10.2 Gurudumu la Usalama

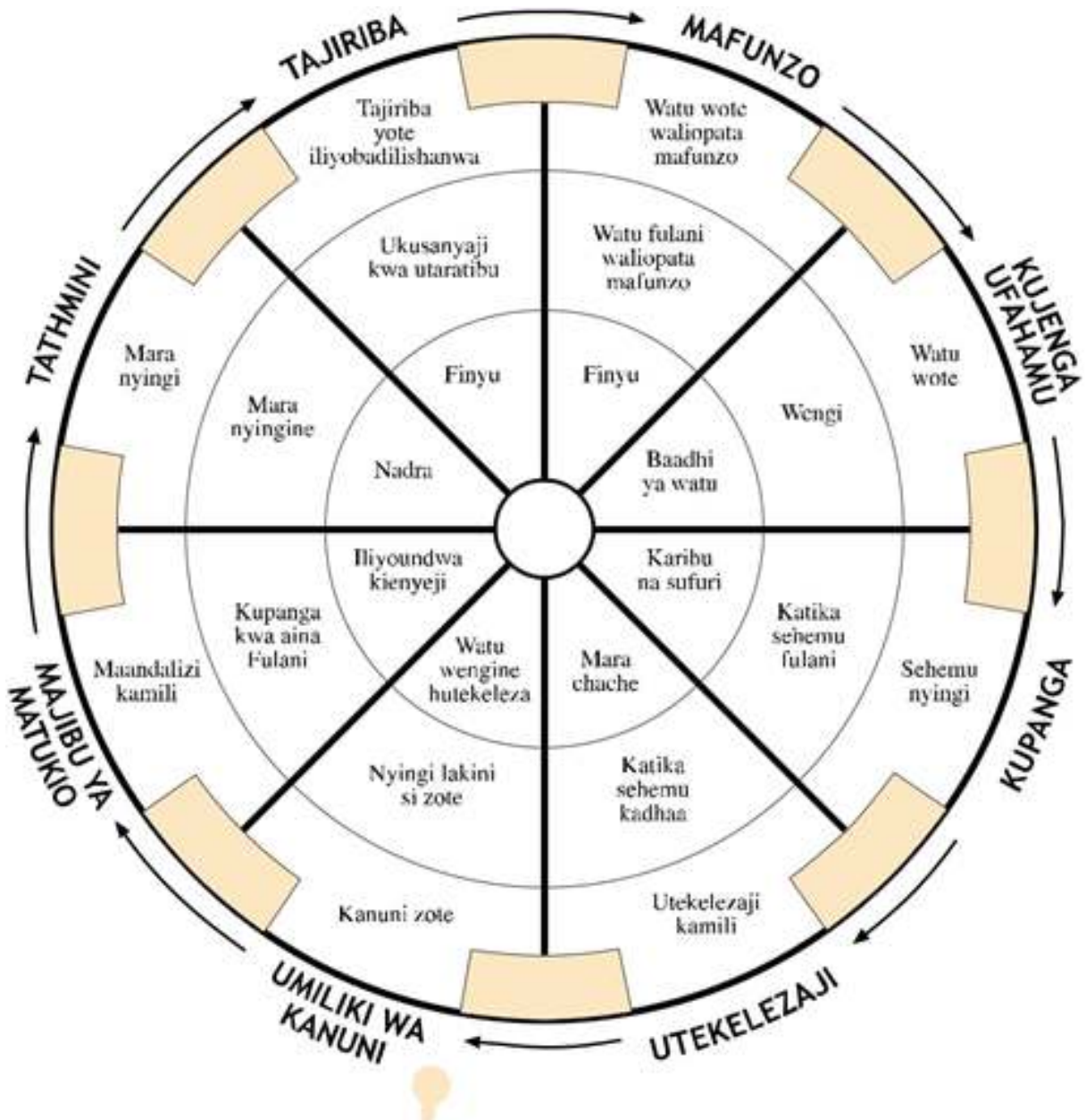
Ufuatiliaji wa usalama wa shirika kwa kutumia vigezo sawa unaweza kutekelezwa kwa kuzingatia gurudumu la usalama na sehemu zake nane. Mantiki ni kwamba gurudumu lazima liwe na usawa pande zote ili liweze kuzunguka; kwa maneno mengine, sehemu zote zinahitajika kuwa za urefu sawa. Hali hiyo inatumika katika gurudumu la usalama na sehemu zake 8 (vipengele) vinavyowakilisha usimamizi wa usalama katika shirika au kikundi cha watetezi.

Tathmini hii inaweza kufanyika kwa makundi ya watendaji wote katika shirika kama ifuatavyo:

i. Chora Mchoro wa gurudumu
ii. Jaza nafasi kila sehemu kulingana na jinsi unavyofikiri ni sahihi na halisi
iii. Andika sababu (tafakari) kwa nini baadhi ya sehemu maalum zimejazwa kidogo kulinganishwa na sehemu zenye ujazo mkubwa, orodhesha njia ulizotumia kufikia matokeo hayo na kuweka malengo na taratibu husika na kuonyesha ufumbuzi.
iv. Mara baada ya kumaliza zoezi hili, tunza salama nakala ya gurudumu lako na rudia zoezi baada ya miezi michache. Utakuwa na uwezo wa kulinganisha magurudumu mawili na kuamua uhakika na hatua ikiwa mambo yamebadilika.

Sampuli ya gurudumu la usalama

Gurudumu la usalama ni nadra kuwa kamilifu: Vipengele vingine vinaujazo zaidi kuliko vingine. Kwa hiyo ni muhimu kuamua kiwango cha ujazo wa kila sehemu. Kwa njia hii, unaweza kutambua ni mipango gani ambayo inahitaji kupitishwa ili kuboresha ulinzi na usalama wako na shirika.



Chora gurudumu kwenye chati, paka rangi kwenye sehemu za ndani kuelezea sura halisi ya gurudumu kwa kundi lako au shirika. Basi utaweza kwa urahisi kuona vipengele ambavyo vimejazwa zaidi -na ambavyo vimejazwa kwa kiwango cha chini.

Sura ya

11

Kuunda na Kutekeleza Mpango wa Usalama

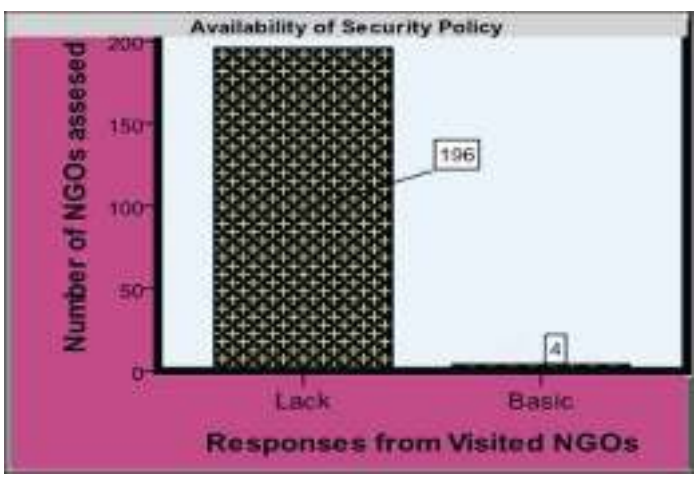
11.0 Utangulizi

Mpango wa usalama ni hati ambayo inajumuisha hatua za kinga na kukabiliana na masuala yote ya usalama na ulinzi ambayo huimarisha ulinzi na usalama binafsi na wa shirika. Huu ni mpango na mkakati wa ulinzi na usalama wa shughuli zote za shirika, wafanyakazi, na wadau wengine.

11.1 Tofauti kati ya Sera ya Usalama na Mpango wa Usalama.

Sera ya usalama ni jumla ya kanuni na miongozo ndani ya shirika ili kukidhi mahitaji ya usimamizi sahihi wa usalama. Mpango wa usalama unaweza pia kuzingatia utekelezaji wa sheria, kanuni, na miongozo hiyo kwa lengo la kuendana na hali husika katika kipindi fulani au shughuli fulani inayofanywa na shirika. Kwa mfano, shirika linaweza kuunda mpango wa usalama huku likijitayarisha kwenda kwenye uchunguzi kwa vitendo na kuweka kanuni au sera zinazolenga kushughulikia na kuangalizia suala la usafiri wa wafanyakazi na usalama wao.

11.2 Watetezi wa Haki za Binadamu na mipango ya ulinzi na usalama Tanzania.



Kwa mujibu wa ripoti ya THRDC ya 2013 juu ya tathimini ya mahitaji ya ulinzi na usalama, ni mashirika manne tuu ya haki za binadamu kati ya mashirika 200 yaliyoshiriki katika tathmini hii ndiyo yaliyokuwa na Sera ya ulinzi na usalama pamoja na mipango iliyoandaliwa vyema, kanuni, sheria na majukumu mashirika hayo manne yalikuwa Action Aid Zanzibar, Care international Mwanza, OXFAM -Arusha na DONET huko Dodoma.

Mchoro hapo juu unaonesha mashirika ya haki za binadamu 196 yaliyotathiminiwa kuwa hayana Sera ya ulinzi na usalama au mpango wowote unaohusu usalama wao. Hadi wakati ambao Muongozo huu wa usalama na ulinzi unaandikwa, zaidi ya mashirika 10 ya utetezi wa haki za binadamu yana Sera ya ulinzi na mipango. Baadhi ya mashirika hayo ni Chama cha Wanasheria Wanawake Tanzania (TAWLA), Mtandao wa Programu ya Jinsia Tanzania (TGNP), Shirika la Kutetea hazi za watu wenye ualbino (UTSS), Mtandao wa kushughulikia masuala ya uzazi na madhara ya utoaji mimba usio salama (CAMMAC) na Kituo cha Sheria na Haki za Binadamu (LHRC) kwa kutaja machache kati ya yote.

11.3 Namna ya kuunda Mpango wa Usalama.

Ili kuandaa mpango wa usalama, wafanyakazi wanapaswa kukutana na kutoa mawazo yao kupitia majadiliano ya pamoja ya usalama. Kama mmekwishafanya tathimini ya hali ya hatari katika Shirika lenu, mtakuwa tayari mmeweza kufahamu orodha ndefu ya mambo hatarishi, hofu, woga, wasiwasi aina kadha ya vitisho na orodha ya njia za kukabiliana navyo.

i. Chagua vitisho vichache.

Panga kwa orodha ya vitisho hivyo kwa njia ya vipaumbele au viweke kwa mpangilio na daraja kufuatia uzito wake, tumia moja ya vigezo hivi: Vitisho vikali zaidi vya kutishia kifo, kwa mfano;

Hali ya kuweza kutokea vitishio vikubwa zaidi na vikali - ikiwa mashirika sawa na yako yameshambuliwa, hilo ni tishio la wazi na la kipaumbele katika chaguo lako; au tishio ambalo limetokea katika shirika sawa na lako na linatoa wasiwasi na hofu kama iliyokatika shirika lako sababu ya kuwa na wewe upo katika hali hatarishi kutokana na uwepo wa tishio la namna hiyo.

ii. Orodhesha

Wasiwasi, hofu ambazo zinatokana na vitisho ambavyo umeviorodhesha.

Hofu na wasiwasi vinapaswa kushughulikiwa kwanza, lakini kumbuka kuwa sio wasiwasi na hofu zote zinahusiana na vitisho vyote. Kwa mfano; ikiwa unapata au kupokea vitisho vya kifo, inaweza kuwa sio muhimu sana kuanza kukarabati, kuimarisha na kulinda kabati lako la ofisi ili kuzuia uvamizi katika ofisi yako iliyo katikati ya jiji (isipokuwa kama unaweza kushambuliwa kwa urahisi katika ofisi, ambayo sio kawaida).

Bali inaweza kuwa muhimu zaidi kwa kupunguza kukaa na kutembea bila ulinzi hasa wakati wa kutoka nyumbani kwenda ofisini au siku za mapumziko. kulinda na kuimarisha makabati ya ofisini yanayotumika kuhifadhia nyaraka sio kwamba sio muhimu ni muhimu pia ila hii haitapunguza hofu na wasiwasi wako ya vitisho vya kifo unavyopokea.

(iii) Orodhesha uwezo wa utatuzi ambao unao wenye kuhusiana na vitisho ulivyo viorodhesha.

Sasa utakuwa katika nafasi ya kupambana vitisho vilivyo orodheshwa, wasiwasi, hofu na uwezo wa utatuzi na kukabiliana katika mpango wako wa usalama, na kwa namna hiyo inawezekana kabisa kwamba utapunguza hali yako hatarishi kupitia njia hizi.

Tafadhali, fahamu kwamba hii ni njia moja ya haraka au ya ziada ya kuandaa mpango wa usalama. Kuna njia rasmi nyingi za kuandaa mpango wa usalama ila mbinu hii ni rahisi na ya kueleweka na ina hakikisha una fanyia kazi masuala nyeti kwa haraka na usalama. Inafanya thamini yako ya hatari kuwa sahihi, na mwisho kuishia kukupa mpango imara na halisia, ambao ndio sehemu muhimu ya usalama.

11.4 UTEKELEZAJI WA MPANGO WA USALAMA.

Mipango ya usalama ni muhimu ,ila sio rahisi kuitekeleza .utekelezaji wake ni zaidi ya mchakato wa kimbinu (technical process),ni mchakato wa kitaasisi, kishirika na kijumuiya na unahitaji uhusishaji na ushirikishwaji wa wafanyakazi wote,na uungwaji mkono wa menejimenti yote ya shirika. Pia unahitaji uwepo wa mawasiliano miongoni mwa wote waliohusishwa katika uandaaji wake kwa mujibu wa maudhui. Kuwe na hatua za kuhakikisha nia ya dhati ya utekelezaji, kuipitia mipango hiyo mara kwa mara ili iendane na wakati husika.

Hii ina lengo la kutafuta mkakati, fursa na vikwazo na matatizo katika mipango hiyo ya usalama wakati wa utekelezaji.

- Mpango usalama unapaswa kutekelezwa katika ngozi kuu tatu.
  i. Ngazi ya mtu mmoja mmoja. Kila mtu ana takiwa kufuata mpango usalama ili uweze kufanya kazi.
  ii. Ngazi ya shirika. Shirika lote kwa ujumla linatakiwa kufuata mpango huo.
  iii. Ngazi ya Shirika na Shirika

Hii hutokea pale ambapo shirika na shirika linaingia ushirikiano miongoni mwao mpango wa usalama mara nyingi ni muhimu pia kuuhusisha ili kulinda usalama.

Mifano ya mikakati na fursa wakati wa utekelezaji wa mpango wa usalama;

- Pale ambapo suala dogo la kiusalama limetokea katika shirika lako au shirika lingine na wafanyakazi wanaingiwa na hofu hii hufanya wazidi kuwa makini zaidi.
- Kutokea kwa suala linalohusu usalama kwa ujumla kutokana hali fulani ilivyo nchini.
- Mfanyakazi mpya anayeanza kazi anaweza kufundishwa kuanza masuala ya usalama vizuri na kwa urahisi zaidi.
- Shirika lingine linapokupa msaada wa mafunzo ya usalama.

Mifano m ya matatizo na vikwazo wakati wa utekelezaji wa mpango wa usalama.

- Watu hudhani kuchukua hatua za kiusalama zitapelekea mzigo wa majukumu katika shirika.
- Wengine hufikiri huwa shirika tayari lina usalama na ulinzi wa kutosha.
- Wengine wamejikita katika shughuli zao na kupuuzia masuala ya usalama.

Hudhani kuwa mambo ya usalama sio kwaniaba ya shirika ila ni kwa niaba ya watu wanao kusudiwa kusaidiwa.

Sura ya

12

Usalama na Namna ya Kudhibiti Msongo wa Mawazo

12.0 Utangulizi.

Mara nyingi kwenye sehemu ya kazi mawazo na huzuni ni kawaida. Mawazo na huzuni kupita kiasi zinaweza kuingilia utendaji wako na uwezo wako kazini, huathiri afya yako ya kimwili na ya kihisia, na kuathiri mahusiano yako na maisha ya nyumbani. Inaweza hata kumanisha tofauti kati ya mafanikio na kushindwa katika utendaji wa kazi. Huwezi kudhibiti kila kitu katika mazingira yako ya kazi, lakini hiyo haimaanishi kuwa hauna uwezo wa kuzuia wakati unakabiliwa na hali ngumu na matatizo.

Kwa hali yeyote ya matakwa yako au mahitaji ya kikazi, kuna hatua ambazo unaweza kuchukua ili kujilinda kutokana na madhara mabaya ya huzuni na mawazo, kuboresha ufanisi wa kazi yako, kuimarisha ustawi wako ndani na nje ya kazi. Watetezi wa Haki za Binadamu kama kundi lolote la watu wanakabiliwa na mawazo na huzuni kwa sababu ya kazi zao. Kwa hiyo muongozo huu utasaidia mbinu za kupunguza na / au kuzuia mawazo na huzuni kwa watetezi.

12.1 Ni wakati gani mawazo na huzuni hutamalaki sehemu ya kazi?

Kuwa na mawazo sio jambo baya mara zote. Mawazo kidogo yanaweza kukusaidia kukaa kwa umakini, kuwa na nguvu, na uwezo wa kukabiliana na changamoto mpya mahali pa kazi.

Ndicho kinacho kupa umakini wakati wa uwasilishaji au tahadhari ili kuzuia matukio yenye madhara, ajali au makosa makubwa. Lakini katika dunia ya leo yenye hekaheka mahali pa kazi mara nyingi huonekana kama sehemu yenye kuongeza hisia na mawazo kutokana na kufanya kazi kwa muda mrefu, kupewa ukomo mfupi wa kumaliza kazi fulani, na hata ongezeko la mahitaji yote haya yanaweza kukuacha na wasiwasi. Hofu na kukumbwa na mambo mengi na pindi mawazo na huzuni vinapozidi uwezo wako wa kuhimili unapungua na huanza kukusababishia madhara ya mwili, kiakili na kutoridhika na kazi unayoifanya.

Ikiwa mawazo katika kazi zako huingilia utendaji wako wa kazi, afya, au maisha ya binafsi, ni wakati wa kuchukua hatua.

Haijalishi unafanya nini kwa ajili ya kuishi, au jinsi gani kazi yako inavyosababisha mawazo, kuna vitu vingi ambavyo unaweza kufanya ili kupunguza kiwango cha mawazo yako yote na kurejesha hisia za udhibiti wa kazi kikamilifu.

12.2 Vidokezo vya kukabiliana na mawazo.

(a) Shinda mawazo sehemu ya kazi kwa njia ya kushirikisha wenzako kwa msaada wa kimawazo.

Muda mwingine njia bora ya kupunguza mawazo ni kushirikisha mtu aliyekaribu na wewe. Tendo la kuzungumza na kupata msaada uso kwa uso inaweza kuwa njia yenye ufanisi sana ya kuepuka hisia na mawazo na kurejesha hali yako ya utulivu. Mtu mwingine hawezi kutatua matatizo yako; anahitaji tu kuwa msikilizaji mzuri.

(b) Rudi kwa wafanyakazi wenzako kwa msaada. Kuwa na mfumo mzuri wa msaada katika kazi inaweza kusaidia kukuzuia athari mbaya za kimawazo katika kazi yako.

Kumbuka tu kuwasikiliza na kutoa msaada wakati wanahitaji msaada pia. Ikiwa huna rafiki wa karibu kwenye kazi, unaweza kuchukua hatua za kuwa mchangamfu zaidi kwa kila mfanyakazi mwenzako. Unapopumzika, kwa mfano, badala ya kuelekeza mawazo katika simu yako, jaribu kushirikiana na wenzako.

(c) Tegemea marafiki na familia yako. Pamoja na kuongeza mahusiano ya kijamii na watu wa kazini. kuwa na mtandao imara wa marafiki na familia ni muhimu sana kudhibiti mawazo katika maeneo yote ya maisha yako.

Kwa upande wa mwingine namna unavyokuwa mpweke au mwenye kujitenga ndivyo unapozidisha kuwa na wasiwasi na udhoofu kuendelea kuwa na mawazo.

(d) Jenga urafiki mpya wenye kuridhisha. Ikiwa hujisikii kuwa na mtu yeyote wa kumfuata au kuwa nae karibu kazini

Hujachelewa sana kujenga urafiki wapya. kutana na watu wapya wenye fikra sawa na wewe kuwa nao pamoja ,toa muda wako kuwa nao karibu , Pamoja na kuwa na njia nzuri ya kupanua mtandao wako wa kijamii, kuwa mwepesi kusaidia wengine hasa wale ambao ni wenyekufurahishwa na wenyekutoa shukrani ,katika hali ya kusaidia na kutoa msaada inaweza kusaidia kupunguza mawazo.

(e) Saidia afya yako mazoezi na lishe.

Unapofanya jikita sana katika kazi, ni rahisi kupuuza afya yako ya kimwili. Lakini wakati unasaidia afya yako na lishe bora na mazoezi, unapata nguvu zaidi ya kukabiliana na mawazo. Kujijali mwenyewe haihitaji kubadilisha mfumo mzima wa maisha yako, hata mambo madogo madogo yanaweza kuinua furaha na hali yako, huongeza nguvu zako, na kukufanya uhisi kama unarudi katika hali yako ya kawaida.

(f) Tenga muda wa zoezi ya viungo mara kwa mara.

Mazoezi ya kutosha ya viungo yanayofanya mapigo ya mayo kuwa imara na kutokwa jasho-ni njia nzuri sana ya kuinua furaha yako na utulivu wa kiakili, huongeza nguvu, kuimarisha umakini wa hali ya juu, hufanya kuwa imara kiakili na kimwili.

Pia kutembea, kukimbia, kucheza, kupiga ngoma ni muhimu sana sababu hulainisha mfumo wa neva.

Ili kuwa na faraja ya kimawazo, jaribu kupata angalau dakika 30 za kupumzika wakati ukiendelea na shughuli zako za siku.

Ikiwezekana kabisa weka katika ratiba yako ya kazi muda mfupi wa kupumzika kama vipindi vitatu vya kupumzika wakati ukifanya shughuli zako za siku.Na pindi mawazo yakiendelea zaidi na kuathiri utendaji wako wa kazi, Jaribu kupumzika haraka, na tembea jinyooshe na toka sehemu yenye mawazo, toka nje ya sehemu ya kazi tembea tembea kama inawezekana kitendo cha kutembea tembea kutoka sehemu moja na nyingine hufanya upate nguvu mpya na urejee katika hali yako.

Namna unavyo chagua chakula chako inaweza kuwa na athari kubwa sana utakavyojihisi wakati wa uwapo kazini kula kidogo ila chakula chenye afya kwa mfano, inaweza kukusaidia mwili wako kudumisha kiwango cha chini cha sukari katika damu hukufanya kuwa na nguvu na kuwa na umakini na hukuepusha na hisia zisizo za lazima,

Kiwango cha chini cha sukari katika damu, kwa upande mwingine, kinaweza kukufanya uhisi wasiwasi na hasira, wakati kula sana kunaweza kukufanya uwe dhaifu, dhoofu na mwenye uchovu na uvivu.

(g) Kula kiafya.

Kupunguza sukari na kiwango cha wanga mara nyingi mtu akiwa na mawazo unakuta anapenda au kuomba vyakula viyamu vyenye kiwango cha sukari kama, bidhaa za kuokwa, au vyakula virahisi tuu kama tambi na chipsi ila vyakula hivi hupelekea kudhoofisha mwili, kuongezeka kwa hisia na kuishiwa nguvu na hufanya hali ya kuwa na huzuni na mawazo kuzidi kuliko kupungua.

- Kupunguza ulaji wa vyakula ambavyo vinaweza kuathiri hali yako, kama vile kahawa, vyakula vya mafuta, na vyakula vilivyo na viwango vya juu vya kemikali au homoni.
- Epuka nikotini.
- Kuvuta sigara unapohisi kuwa mwenye mawazo kunaweza kukufanya kuonekana mtulivu lakini nikotini ina nguvu ya msisimko hupelekea uwoga na hofu kwa kiwango cha juu na sio cha chini.
- Kunywa pombe kwa kiasi.
- Pombe inaweza kuonekana kupunguza wasiwasi na hofu kwa muda mfupi, lakini matumizi makubwa ya pombe yanaweza kusababisha wasiwasi na hofu kwa kiwango kikubwa na huathiri hali yako uliyo nayo.

h) Usiruke muda wa kulala.

Unaweza kujisikia kama huna muda wa kupata usingizi usiku mzima, lakini kulala muda mchache kuliko kawaida kunaathiri majukumu yako ya siku ubunifu, uwezo wa kutatua matatizo na uwezo wa umakini utakavyo pumzika muda wa kutosha, ndivyo utakavyoweza kuwa makini na kufanya majukumu yako vyema na vizuri na kuweza kukabiliana na changamoto za sehemu ya kazi.

Boresha ubora wa usingizi wako kwa kufanya mabadiliko ya kiafya katika majukumu yako ya mchana na usiku. Kwa mfano, lala usiku na uamke kwa wakati mmoja kila siku katika maisha yako hata wakati wa mwisho mwa wiki kuwa makini juu ya unacho kula ns kunywa kila siku, na ufanye marekebisho kwenye mazingira yako ya kupumzikia, Lengo ni la masaa 8 ya kupumzika usiku - kiasi cha usingizi ambacho wazima wanakihitaji ili kufanya kazi kwa bora zaidi.

- Zima TV, simu yako au kompyuta yako saa moja kabla ya kulala. Kwa sababu nuru inayotokana na TV, simu ya mkononi, na kompyuta zinazuia uzalishaji wa melatonin katika muili wako hivyo huweza kuharibu kabisa usingizi wako.
- Epuka shughuli chochezi na zenye hali ya kuwazisha kabla ya kulala usiku, kama vile kufanya kazi ambazo zingefanywa mapema,

  Badala yake, jikite katika mambo ya utulivu na yasio chosha, kama vile kusoma na kusikiliza musiki, huku mwanga ukiwa wa chini.

(i) Kipaumbele na kuandaa.

Pindi mawazo ya kazi na mahali pa kazi yanakuandama kuna hatua za vitendo za kuchukua to kudhibiti hali.

- Unda ratiba yenye usawa kuwa kila kazi au majukumu ni ya msingi hakuna lisilo la msingi, Jaribu kupata usawa kati ya kazi na maisha ya familia, shughuli za kijamii na shughuli za faragha, majukumu ya kila siku na Muda wakati wa kupumzika.
- Ondoka mapema asubuhi. Hata dakika 10-15 inaweza kuleta tofauti katika siku yako nzima, aidha ufanye kazi kwa harakaharaka au ufanye kazi kwa utulivu, Ikiwa kila siku unachelewa, tega muda wako au saa ili kujipa muda wa ziada kwa lengo la kupunguza haraka haraka na mawazo katika kufanya majukumu yako.
- Panga mapumziko ya kila mara. Hakikisha kuchukua mapumziko mafupi wakati wote wa majukumu yako ukiwa kazini mfano. kutembea, kuzungumza kwa uso wa upole, au ufanyie mbinu ya kufurahi. Pia jaribu kuondoka ofisini na utoke kwenda kula nje. Itasaidia kupumzika na kurejesha nguvu na uimara zaidi.
- Kuanzisha mipaka mizuri. Wengi wetu hawaweki mipaka na matokeo yake masaa yote 24 kwa siku unakuta anaendelea kufanya kazi kupitia simu yake, kupata jumbe fupi za kikazi hata akiwa nyumbani, Lakini ni muhimu kudumisha wakati usiofanya kazi au kufikiri juu ya kazi. Hii ina maanisha kuwa usiangalie barua pepe au kupokea simu za kiofisi ukiwa nyumbani jioni, au siku za mwisho wa wiki.
- Usijitoe zaidi. Epuka kupanga ratiba zinazojirudia rudia. Ikiwa umepata majukumu mazito ni vyema kutofautisha “kupaswa” na “lazima” achana na majukumu ambayo sio ya lazima katika orodha na uyaondoe kabisa.

(j) Vidokezo vya usimamizi wa kazi kwa kupunguza mawazo katika kazi.

- Weka Kipaumbele katika shughuli zako, Fanya kwanza kazi za kipaumbele cha juu, Ikiwa una kazi ambayo ni ngumu au sio nzuri ifanye mapema zaidi, na kazi zote zitakazo baki kwako zitakuwa nyepesi.

- Gawa miradi au majukumu yako katika hatua ndogo. Ikiwa mradi au kazi kubwa inaonekana kukuchosha. Fanya kila uliwezalo kwa hatua badala ya kufanya yote kwa pamoja.
- Gawa majukumu kwa wengine. Hupaswi kufanya kila kitu wewe mwenyewe. Epuka kutamani kufanya kila jambo kwa namna hiyo utachana na mawazo yasio ya msingi katika mchakato.
- Kuwa tayari kujiweka kawaida. Wakati mwingine, ikiwa wote mnaweza kujishusha kidogo muwapo kazini wote mtaweza kupata furaha na hii itapunguza kiwango vya mawazo kwa kila mtu wenu.

(k) Achana na tabia mbaya ambazo zinachangia mawazo mahali pa kazi.

Wengi wetu hufanya kazi kuwa mbaya zaidi kutokana na mawazo na tabia mbaya.

Ikiwa unaweza kukabiliana na tabia hizi binafsi na kuzishinda, unaweza kuta muajiri anakusababishia mawazo au shida ambazo unaweza kuzidhitbiti kwa urahisi sana.

- Pinga ukamilifu. Unapojiwekea malengo yasiyo ya kweli, unajisababishia kushindwa lenga kufanya vizuri zaidi. Hakuna mtu anayeweza kuomba zaidi ya kufanya vizuri zaida
- Ondoa mawazo yako hasi. Ikiwa utajikita kuwaza kushindwa katika kila jambo na mwingiliano, utajikuta mwenyewe unaishiwa nguvu na hamasa. Jaribu kufikiri chanya kuhusu kazi yako, jaribu kuepuka wafanyakazi wenza wasio na mawazo chanya jiweke nyuma ya majukumu madogo madogo hata kama hakuna mtu mwingine anayefanya.
- Usijaribu kudhibiti tabia isio dhibitika.

  Vitu vingi kazini hatuwezi kuvidhibiti ni zaidi ya uwezo wetu hasa tabia za watu wengine, tunashindwa kudhibiti vyema badala yake tunawasababishia mawazo, fikiria mambo ambayo unaweza kudhibiti kama vile unavyochagua kushughulikia matatizo.
- kuwa na hali ucheshi na furaha katika hali hiyo. Wakati unatumiwa ipasavyo katika majukumu yako, ucheshi ni njia nzuri ya kupunguza matatizo na mawazo katika sehemu ya kazi. Wakati wewe unapoanza kuchukua mambo kwa uzito sana, tafuta njia ya kupunguza uzito huo kwa kushirikiana na rafiki zako kicheka na kutaniana pamoja.
- panga na weka matendo na vitu vyako sawa. Ikiwa meza yako au nafasi yako ya kazi ni chafu, safisha na ondoa uchafu wote uliopo mezani kwako kwa kazi; kujua tu namna gani kitu kinaweza kuokoa muda na kupunguza mawazo.
- Kuwa zaidi ya makini na imara katika kazi yako na majukumu yako ya kiofisi na mahali pa kazi. Unapojisikia vibaya wenye mawazo wasio na uwezo wa kudhibiti mawazo hayo kwa kiwango kikubwa

Hapa kuna baadhi ya mambo unayoweza kuyafanya ili upate upya hisia ya udhibiti juu ya kazi yako na majukumu yako.

- Ongea na mwajiri wako kuhusu wasiwasi na shida za sehemu ya kazi Wafanyakazi wenye afya na wenye furaha wanaozalisha zaidi, hivyo mwajiri wako ana wajibu wa kudhibiti matatizo yaliyopo sehemu ya kazi wakati wote inapowezekana. Pia vyema kuorodhesha malalamiko na matatizo yaliyopo sehemu ya kazi ili mwajiri wako ajue kuhusu hali maalum ambazo zinaathiri utendaji wako wa kazi.
- Fahamu maelezo na ufafanuzi wa kazi yako. Muombe msimamizi wako kwa maelezo mapya ya kazi na majukumu yako. Pia unaweza kutenga na kuchagua kufanya kazi ambazo sio sehemu ya maelekezo au ufafanuzi wako wa kazi, ili kupata kungwa mkono na kuonekana muwajibikaji kwa kuonesha kuwa ukifanya majukumu zaidi hata ya yale yalio katika ufafunuzi na muongozo wa kazi zako.
- Omba uhamisho. Ikiwa eneo lako la kazi ni kubwa sana, unaweza kuepuka mazingira mabaya kwa kuhamishwa kwenye idara nyingine.
- Omba kazi mpya. Ikiwa umekuwa ukifanya kazi hiyo hiyo kwa muda mrefu, omba kujaribu kitu kipya: katika kiwango cha daraja tofauti, eneo la kazi tofauti, na utendaji tofauti.
- Chukua muda wa mapumziko nenda likizo, tumia siku zako za ugonjwa, uomba kuondoka kwa muda mfupi. Tumia muda huo kurejesha nguvu zako na kuchukua mtazamo mpya.

(i) Jinsi waajiri wanavyoweza kupunguza mawazo na matatizo Kazini

- Shauriana na waajiriwa wako. Zungumza nao juu ya mambo maalum ambayo hufanya kazi zao kuwa ngumu. Vitu vingine, kama vile ubovu wa vifaa, uhaba wa wafanyakazi, au ukosefu wa wawasimamizi. Kubadilishana mawazo na kuhabarishana changamoto kazini kunaweza kupunguza wasiwasi, hofu na mawazo katika kazi na hatima yao.
- Wasiliana na wafanyakazi wako mmoja mmoja wasikilize kwa makini uso kwa uso utafanya wafanyakazi kujisikia kusilizwa na kuelewaka na kusaidia kupunguza matatizo, mawazo yao na yako-hata kama huwezi kubadilisha hali iliyopo.
- Shughulikia migogoro ya mahali pa kazi kwa njia nzuri. Kuheshimukila mfanyakazi; kuanzisha sera ya kutovumilia unyanyasaji.
- Wawezeshe wafanyakazi fursa kushiriki katika maamuzi yanayoathiri kazi zao. Wape wafanyakazi fursa za mawazo yao katika mchakato wa kuandaa sheria na taratibu za kazi kwa mfano. Ikiwa wamehusika katika mchakato huo, watakuwa thabiti na hamasa kubwa.
- Epuka kuweka muda usiofaa kwa wajiri au wafanyakazi juu ya muda wa mwisho (deadlines) kuwasilisha kazi, hakikisha majukumu unayoyatoa yanaendana na uwezo wa wafanyakazi na vitendea kazi na rasilimali.
- Eleza matarajio yako fafanua waziwazi wajibu, majukumu, na malengo ya wafanyakazi. Tengeneza vitendo vya usimamizi vizuri na thabiti vyenye kuenda sambamba na maadili ya shirika.
- Kutoa tuzo na zawadi kama motisha. Sifu utendaji mzuri wa kazi kwa shirika kwa ujumla. Weka ratiba ya kipindi kigumu chenye majukumu mengi ikifuatiwa na kipindi chenye majukumu machache yasio bana sana. Toa nafasi kwa wafanyakazi kukutana na kushirikiana kwa kukutanishwa kwa masuala ya kijamii.

Marejeo na viunganisho vya msingi.

1. Kitabu cha ulinzi wa watetezi wa haki za Binadamu 2005, kimeandaliwa na watetezi wa haki za Binadamu
2. Ripoti ya hali ya watetezi wa haki za Binadamu nchini Tanzania, 2013,2014,2015,2016, na 2017 imeandaliwa na Mtandao wa watetezi wa haki za Binadamu.
3. Muongozo wa usalama kwa watetezi wa haki za Binadamu barani Afrika, 2017 imeandaliwa na watetezi wa haki za Binadamu.

Viunganisho muhimu.

http://locdoc.net/security-and-locksmithing-blog/8-simple-steps-youcan-take-to-improve-your-office-security-today/

https://www.helpguide.org/articles/stress/stress-in-the-workplace. htm

https://www.apa.org/helpcenter/work-stress.aspx

https://security.berkeley.edu/resources/best-practices-how-toarticles/top-10-secure-computing-tips

https://www.zdnet.com/article/simple-security-step-by-step-guide/

https://www.theguardian.com/technology/2013/sep/16/10-wayskeep-personal-data-safe

https://www.afgonline.com.au/learn/home/top-10-tips-to-improveyour-home-security/

Orodha ya Sheria

Sheria ya Makosa ya Mtandao 2015

Sheria ya Huduma za Vyombo vya Habari, 2016

Sheria ya Upatikanaji wa Taarifa, 2017

Kanuni za Maudhui ya mtandaoni, 2018

Sheria ya Jeshi la Polisi na Huduma Saidizi 1969.

Sheria ya Tawala wa Mikoa, 1997

TANZANIA HUMAN RIGHT DEFENDERS COALITION (THRDC)
Eyasi Road, Near Hekima Garden, P.o.box 105926, Dar Es Salaam, Tanzania
+255 769 64220
thrddefenders@gmail.com
www.facebook.com/TanzaniaHumanRightsDefendersCoalition
www.thrd.or.tz