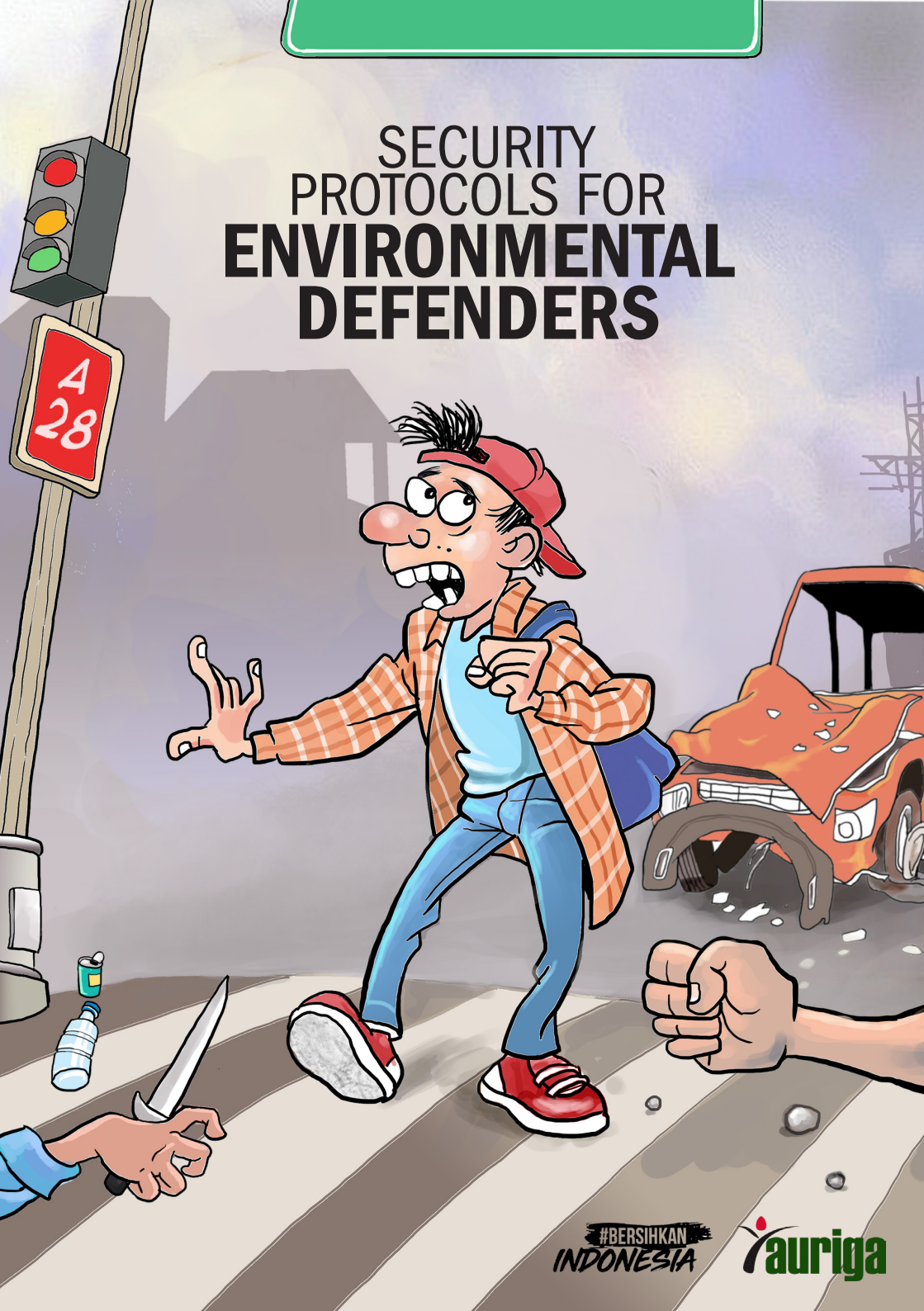
SECURITY PROTOCOLS FOR **ENVIRONMENTAL DEFENDERS**



#BERSIHKAN INDONESIA

auriga

CITATION
Bersihkan Indonesia. 2020. Security Protocols for Environmental Defenders. Jakarta, Indonesia.

@Auriga Nusantara

INTRODUCTION

Violence, torture, denigration of human dignity, and punishment without basis are prohibited acts and constitute serious human rights violations.

As human rights workers, environmental defenders are not infrequently subjected to violence and torture; often resulting in death. Criminalization is a method frequently used by state authorities and other actors.

The government already affords legal protections for environmental defenders in Indonesia, but these only apply to those who fight using legal channels, criminal reports, or civil or state administrative court claims. Beyond these, there are no protections from the state.

Therefore, strategic steps are necessary to ensure the safety and security of environmental defenders when carrying out their work in defending the environment.

RISK ANALYSIS

RISK ANALYSIS

The work of an environmental defender (ED) is full of risks, and specific levels of vulnerability, due to an absence of legal protection from the state. So, we need to stress that risk is an integral part of the life of an environmental defender.

Of course, risk levels are not the same for each environmental defender. They depend on threats and vulnerabilities, and the capacities of environmental defenders and their institutions. Put simply, international protection has established the following formula:

Risk = Threat[1] x Vulnerability[2] : Capacity[3].

In the case of threats, the first thing to do is to assess them. Things you can do when assessing a threat are:

1. Threat constitutes the possibility that someone will endanger the physical or moral integrity, or property of others through violence.
2. Vulnerability is a person's level of susceptibility to loss, damage, suffering and death in an attack.
3. Capacity is the strength and resources possessed by a defender or group for attaining a reasonable level of security.

1. To establish facts surrounding the threat
2. To determine whether the same form of threat exists at different times
3. To ascertain the purpose of the threat
4. To determine the source of the threat
5. To draw a rational and proportional conclusion as to whether of not the threat will actually transpire
6. To react to the threat.

Based on the above, in order to reduce the risk, it is always necessary to record every incident, determine the point person/ security officer responsible for receiving the incident report, and prescribe responses to the incident.

There are so many sectors that need their own security protocols. However, the protocols included here will only cover some of these sectors.


BAR
&
KARAOKE

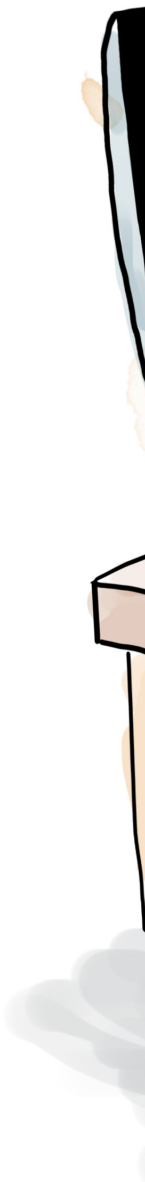
TRAVEL SECURITY PROTOCOLS

TRAVEL SECURITY PROTOCOLS

- Make a travel plan (see Annex 1)
- Carry out checks of all travel documents
- Make Sure of communications access in the destination location
- Recognize routes, be alert to potential high-risk places. Consider alternative routes to avoid criminal activity
- Avoid visits to venues that sell alcoholic drinks
- Be aware of prevailing rules and laws in the places being visited
- Carry out checks of locations/destinations, including important places in case of emergency, such as:
    - The nearest hospital and its telephone number
    - The nearest police station and its telephone number
    - Media contact details.
- For trips using motor vehicles
    - Rental
        - » Identify the vehicle rental owner
        - » Record the model and number plate of the vehicle
        - » Request and record the driver's identity
        - » Inspect the condition of the vehicle

  - » Ensure the driver does not use a telephone during the journey
  - » Do not discuss travel plans with the driver.
- Safety
  - » Do not consume alcoholic drinks.
- Carry out checks of the event venue
  - » Security
  - » Room positions
  - » Emergency doors
  - » CCTV.
- Make a security incident report (see Annex 2)

DATA AND IN-FORM-ATION SECURITY PROTOCOLS




DELETE

DATA AND INFORMATION SECURITY PROTOCOLS

Data and information protocols regulate the classification and handling/treatment of data and information belonging to and managed by an institution where environmental defenders are engaged. In the handling and treatment of data and information, the following are recommended:

1. Knowledge and understanding of the reasons for and aims of the data and information protocols among all environmental defenders, the institution, and those responsible for information
2. Acceptance from everyone involved in the institution
3. If necessary, all information should be marked or labelled
4. Information handling should be carried out in accordance with agreed standards.

Data and information security protocols relate to handling/treatment, storing and deletion.

Data and information include documents, explanations, statements, ideas and signs containing visible, audible and comprehensible meanings and messages presented in various forms and formats, produced, stored and managed by the

institution.

1. GENERAL TREATMENT OF DATA AND INFORMATION

There should be a special team responsible for managing data and preparing forms for data sharing and recording processes

1. Characteristics of data and changes in data characteristics are determined in the institution's annual meetings
2. Classification and codification processes are carried out for all data and documentation gathered
3. Data and document use cover usage for internal and external purposes:
    a. Data and document use for internal purposes is carried out with a form-filling mechanism
    b. Data and document use for external purposes is preceded with the submission of a request by filling in a pre-provided form, recognized by the person in charge, and approved by the institution's management.
4. Data surrendered to external parties should be in PDF file format with all metadata removed.

Data and information managed by environmental defender institutions consist of open access/public, restricted, internal, and closed data and information.

2. OPEN ACCESS DATA AND INFORMATION

Open access information is information that, in principle, is accessible to the public and distributed freely. It can take the form of website content, press releases, publications, activity reports, financial reports, research results and annual reports, as well as other information declared open by law.

3. INTERNAL DATA AND INFORMATION

Internal data and information are those which may only be circulated within the institution and not approved for external distribution. If divulged to the public, they may cause discomfort for people in the institution, and could compromise the implementation of activities and/or cause financial or credibility losses to the institution. However, some internal information could be circulated to the public following approval from the information owner and/or the institution's management. Such internal information might include meeting notes, information about the governors, email content, email addresses, data on institution members, primary financial data, etc.

4. HANDLING/TREATMENT OF INTERNAL DATA/INFORMATION

1. Internal data/information can be accessed freely by everyone working for the institution, but may not be distributed outside the institution
2. There is no requirement to protect internal data/information once it has been sent out through a public network. After securing permission to distribute information, the data/information distributed must be sent in PDF file format with all metadata removed.

STORAGE

1. Internal information can be stored on an internal file server, and may also be stored on a public cloud, depending on the agreed location
2. Physical documentation in filing cabinets, which in principle, can be accessed by all staff members.

DELETION

1. Internal information should be deleted once it is no longer required
2. Internal information relating to personal data should be deleted in accordance with the applicable data storage policy, and carefully deleted.

5. RESTRICTED DATA AND INFORMATION

Restricted information is data and information originating from investigation processing, data that if divulged could compromise the work of environmental defenders, and/or data and information from network work outcomes.

HANDLING/TREATMENT

1. Such data may only be accessed by people holding certain positions within the institution
2. May only be accessed with the prior approval of the institution's management
3. Restricted data and documents must be encrypted.

STORAGE

1. Stored on an internal server
2. Data in hard copy form must immediately be made into softcopy data
3. Physical documents/hard copies should be stored in a special place accessible only to those granted authority from the institution's management.

6. CLOSED DATA AND INFORMATION

Closed information is data and information that is still undergoing work (has yet to be finalized), is confidential, of a compromising nature to the institution's reputation and the work of environmental defenders, as well as data and documentation resulting from investigation processes.

HANDLING/TREATMENT

1. May only be accessed following consideration from the data manager and approval from the institution's management
2. Closed data and documents must be encrypted.

STORAGE

1. Stored on an internal server
2. Data in hard copy form must immediately be made into softcopy data
3. Physical documents/hard copies should be stored in a special place accessible only to those granted authority from the institution's management.


I'M GIVING YOU RESPONSIBILITY FOR THE OFFICE KEYS!

OFFICE SECURITY PROTOCOLS

OFFICE SECURITY PROTOCOLS

Offices are quite sensitive areas. In addition to being workplaces, offices also function as places for storing data and documents. Therefore, office security is an essential consideration.

Things requiring attention are the surrounding environment, whether the building is connected to a person or activity in the past, the availability of private and public transport, accident risks, how suitable the building is for installing security infrastructure, crime statistics, a location safe from disasters and close to places of refuge, and ease of access to the location.

1. OFFICE SELECTION PROTOCOLS

1. For rented office premises, it is necessary to consider the property owner's reputation
2. Consider and understand the surrounding environment
3. At the very least there should be more than one road to access the office
4. The office should have at least 2 (two) access doors, 1 (one) main entrance door, and 1 (one) emergency door used for evacuation
5. Consider the building's structure, facilities for installing

security equipment, doors, windows, access points, garage for parking or a covered area.

2. OFFICE SECURITY PROTOCOLS

1. The office should have at least 2 (two) secure doors/gates that are always kept shut
2. The institution should provide a guest book as a control book containing guests' identities, telephone numbers and purposes of visits
3. Consideration should be paid to guest reception hours
4. Guests should only be given access to a reception room, and not allowed to enter certain rooms, such as data and admin/finance rooms.
5. People/staff may not use the office address for sending or receiving private packets/packages, unless they are given permission to do so by management, and are willing to accept the packet/package being opened beforehand
6. All staff working overtime must report to those responsible for security, or at least have permission from office management
7. Office keys are only provided to those afforded that responsibility
8. To enhance office security, a CCTV system is required, and CCTV data should be backed up monthly
9. As much as possible, the office should be equipped with security guards, fire extinguishers, a generator, a first aid kit, and emergency door
10. The office building and work support inventory must be insured
11. All office items must be inventoried and recorded, and

their condition inspected on a periodic basis

12. Personal use of inventoried items must undergo a lending process with the responsible division
13. Anyone breaking or losing an inventoried office item outside office purposes is obliged to repair or replace the item out of their own pocket
14. Any window facing a road should have a work desk positioned at that window
15. Keep a list of emergency telephone numbers for the police, fire service, ambulance, nearest hospital, other frequently used services, etc.
16. Establish safe locations outside the office for emergency situations
17. Guests may not be left **on their own** in vulnerable places where keys, information or valuable items are accessible
18. Someone must be assigned the responsibility of reviewing office security once every six months.

INSTITUTIONAL REPUTATION SECURITY PROTOCOLS


ON BEHALF OF THE INSTITUTION, I...

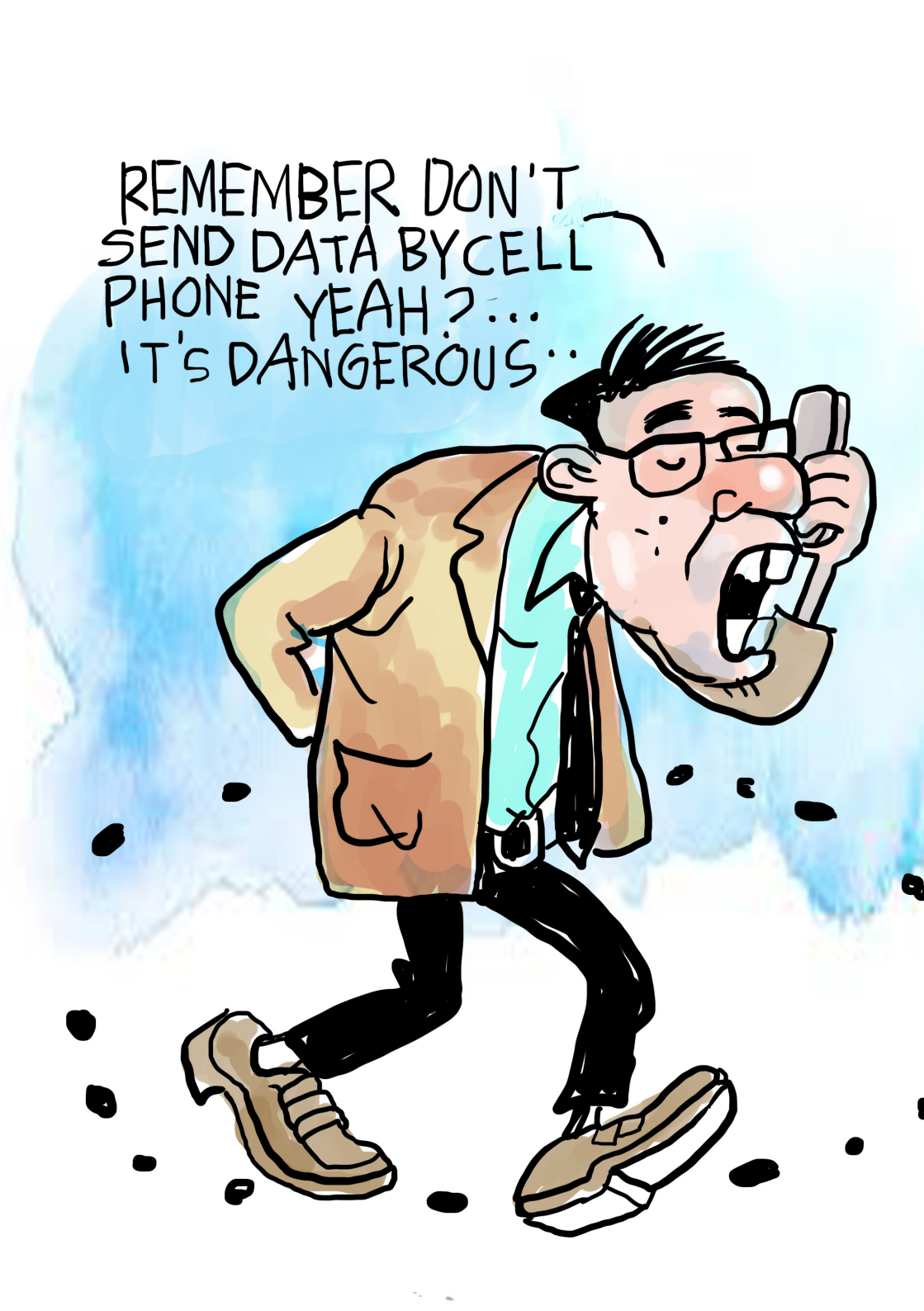
INSTITUTIONAL REPUTATION SECURITY PROTOCOLS

Maintaining the institution's reputation is obligatory for all members of staff. If the institution's reputation is tarnished, it will impact upon and affect public trust. Things applicable to institutional reputation security protocols are:

1. Any environmental defender conducting an investigation is not allowed to reveal their real identity, including their place of work, and is prohibited from posting information and activities on social media
2. To refrain from leaking or transacting data and information belonging to the institution
3. Every institution should have at least one person responsible for ensuring no publications have legal ramifications for the institution
4. Every publication in any form must undergo a peer review from a person granted that responsibility
5. Only one person should be assigned the responsibility of relaying information to the public on the institution's behalf
6. Any use of the institution's logo must secure permission

from the institution's management

7. To apply cautionary principles in collaborative relations with all parties
8. If the office is subject to a search warrant, essential data must have already been safeguarded
9. To be aware of standards and rules surrounding office search warrants
10. For every search, at least one member of staff should observe the process and record every action taken by officers.

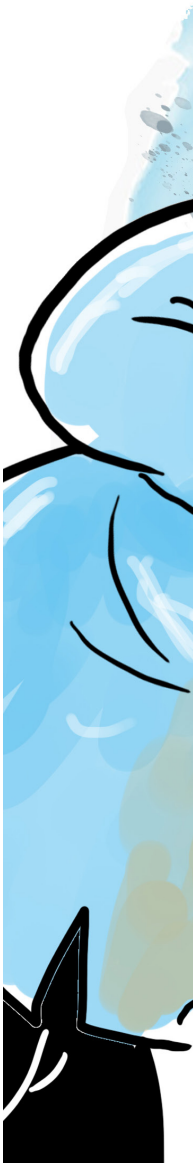

REMEMBER DON'T SEND DATA BY CELL PHONE YEAH?... IT'S DANGEROUS..

COM-
MUNI-
CATIONS
SECURITY
PROTO-
COLS

COMMUNICATIONS SECURITY PROTOCOLS

1. Ensure the use of secure communications channels
2. Prioritize face-to-face meetings to relay things of importance
3. Data should only be sent via email by computer/laptop, and not by smartphone
4. Any data sent that qualifies as important must be encrypted
5. Do not use public Wi-Fi to send important data and information, including to communicate.

PROTO-COLS FOR AD-DRESS-ING CRIMI-NALIZA-TION




HIS BREATH STINKS OF SCORN!

PROTOCOLS FOR ADDRESSING CRIMINALIZATION

Criminalization, as a term, did not use to be a crime, but due to developments it is now considered so. In other terminology, criminalization is also defined as a legal means used by law enforcers to declare someone a criminal on unclear grounds (by looking for mistakes).

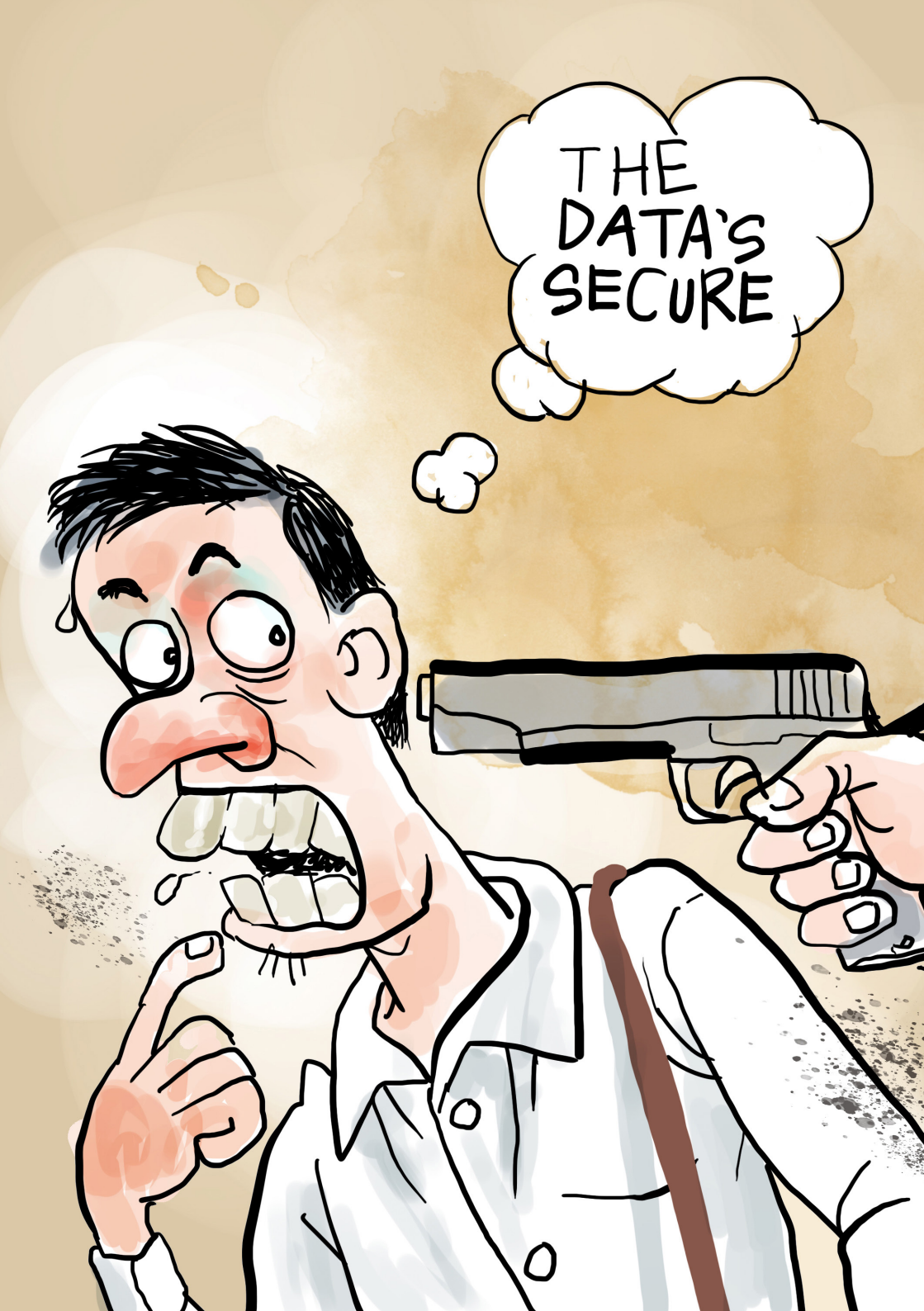
In this second terminology, it is often addressed at activists who defend the rights of communities. Forms of criminalization frequently make use of provisions on defamation, defacement, and provocation.

In order to address this, some things to consider are:

1. Every publication must commence with robust planning; determining content, targets, and the media to be used
2. Each time a publication is made, a threat analysis should be made of things such as criminalization, troll attacks, etc.
3. The content of every publication must be checked by both language and legal experts before being circulated. Data presented in the publication must be from clear

sources, which should be named in the publication where necessary

4. Every action must commence with clear planning and division of duties
5. To be aware of applicable laws and rules
6. To understand the characters of surrounding communities
7. To refrain from using words with the potential to lead to lawsuits, such as insults, false information, and inciting criminal acts
8. In the event of an arrest, three viewpoints should be considered in handling the process: those of the detained party, the institution, and the family
9. An action that should be taken immediately after an arrest is to set up a working group (network) to handle the detention
10. To consider informing other networks to discuss strategic steps to take
11. To identify the detention processes, including the reason for, and the chronology of the arrest
12. To establish a defender/legal adviser network.


THE DATA'S SECURE

PHYS-ICAL THREAT PROTO-COLS

PHYSICAL THREAT PROTOCOLS

In addition to the problem of criminalization, environmental defenders frequently face and experience physical threats. Such threats are usually made by those who do not agree with the cause environmental defenders are fighting for. To cope with this, the following should be done:

1. Every time a trip is undertaken, if possible do not go alone, invite at least one other person.
2. Avoid traveling at night
3. Get to know the work region and places visited
4. Keep all important contact numbers, such as police stations, hospitals, and community health centers
5. Record and report all suspicious occurrences (see Annex 2)
6. Note down perpetrators' features (complete for each perpetrator/suspect): sex, height, build, language, hair, age, race, scars/tattoos/other distinguishing marks, clothes
7. Inventory and store evidence relating to occurrences of physical threat
8. All those granted authority as security persons should give advice on incident reports; whether or not they should be reported to the police.

IN CLOSING

These security protocols are not rigid in nature, but depend on the level of risk, level of threat and capacity of each individual institution/environmental defender. These protocols are very much open for input, revisions and improvements.

(Annex 1)

Travel Plan Form

a. Risk Assessment, b. Security Plan, c. Contact List

Country: .....; Date: .....

RISK ASSESSMENT

1. Aim & Activity

Program:

Objective:

Expected outcome:

2. Travel Plan

This section contains the duration of travel, and the places to be visited

3. Delegate(s)/Participant(s)

The identities of those involved in the trip and the reason(s) for their involvement

4. Contextual Analysis

A brief description of the trip

5. Threat Analysis

A brief description of the security risks and their relevance to participants' security

SECURITY PLAN

6. Delegation Mission, Roles, and Responsibilities

7. Operational Procedures

Explain as standard operating procedures, including for potential sources of threats, and authorities; information and data handling; requirement of visitation, contact person in destination area.

8. Logistics, Accommodation and Transportation

9. Communications and Contact Routines

Equipment:

Contact routines:

10. Medical / Health Provisos

Details of health facilities in the destination location (names, contact details)

Local community health center, place for initial treatment

11. Security Incident Protocols

What actions to take if a security incident occurs

CONTACT LIST

List of relevant contacts, such as telephone numbers for the police, embassy staff, partners

(Annex 2)

Security Incident Report Form

INCIDENT REPORT FORM

TYPE OF INCIDENT (Checklist)

- ☐ Robbery/Theft
- ☐ Attack
- ☐ Vandalism
- ☐ Threat
- ☐ Threatening letter/phone call
- ☐ Injury
- ☐ Death
- ☐ Sexual violence and/or sexual harassment
- ☐ Missing person(s)
- ☐ Police arrest
- ☐ Vehicular accident
- ☐ Vehicle hijacking
- ☐ Shooting incident
- ☐ Raid/ambush
- ☐ Hostage taking
- ☐ Suspicious activity/surveillance
- ☐ Other

INCIDENT LOCATION :
DATE :
TIME :

BRIEF DESCRIPTION :

OUTCOME OF THE INCIDENT

Physical injury: (yes)/(no)

Number of victims:

Treated in hospital: (yes)/(no)

Type of injury:

Victim's name and contact details:

CONDITION OF PROPERTY/EQUIPMENT

Stolen of damaged

PERPETRATOR(S)

Identity of perpetrator(s)/suspect(s) if known
Address, other contact information for the perpetrator(s)/suspect(s) if known
Description of perpetrator(s) (complete for every perpetrator/ suspect): sex, height, build, language, hair, age, race, scars/tattoos/ distinguishing mark, clothes.

WITNESS(ES)

Witness: Full identity

RAPID RESPONSE(S) CARRIED OUT

What emergency response action was taken?
Was/Is an additional response required? If so, what?
Was/Is assistance necessary? If so, what? From whom?

FOLLOW-UP RESPONSE

Report to the police
Were the police informed: Yes/No
Police report attached: Yes/No

PERSON MAKING THE INCIDENT REPORT

Name:
Position in the institution:
Office location:
Email address:
Telephone number:
Date:

(Annex 3)

Office Security Inspection Form

Inspection of :
Conducted by :
Date :

Office security

- *Have office security procedures already been performed?*
- *Are emergency access doors available and can they be used?*
- *Is the guest book being filled in?*
- *Inspect the condition of gates, external fences/walls, doors, windows, walls and rooves, and ensure they are all in working order*
- *Inspect the condition of external lights, alarms, video cameras or telephones at the entrance door, and ensure they are all in working order.*

Guest reception procedures

- *Are reception procedures used for all types of guests?*
- *Are all staff members aware of procedures and do they carry them out properly?*
- *Double check all recorded security incidents that relate to guest reception procedures and 'filters'*
- *Ask all staff that usually receive guests whether the procedures are working well, and what improvements might be needed.*

Safety in the event of an accident

- *Inspect the condition of fire extinguishers, gas valves/pipes and water faucets, electrical plugs, electricity generator and cables (if applicable)*

bersihkanindonesia.org

auriga.or.id