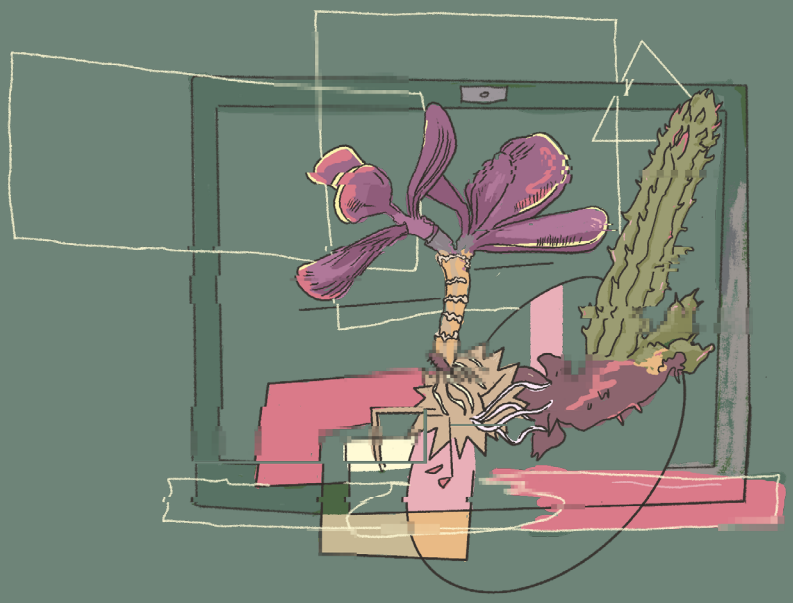
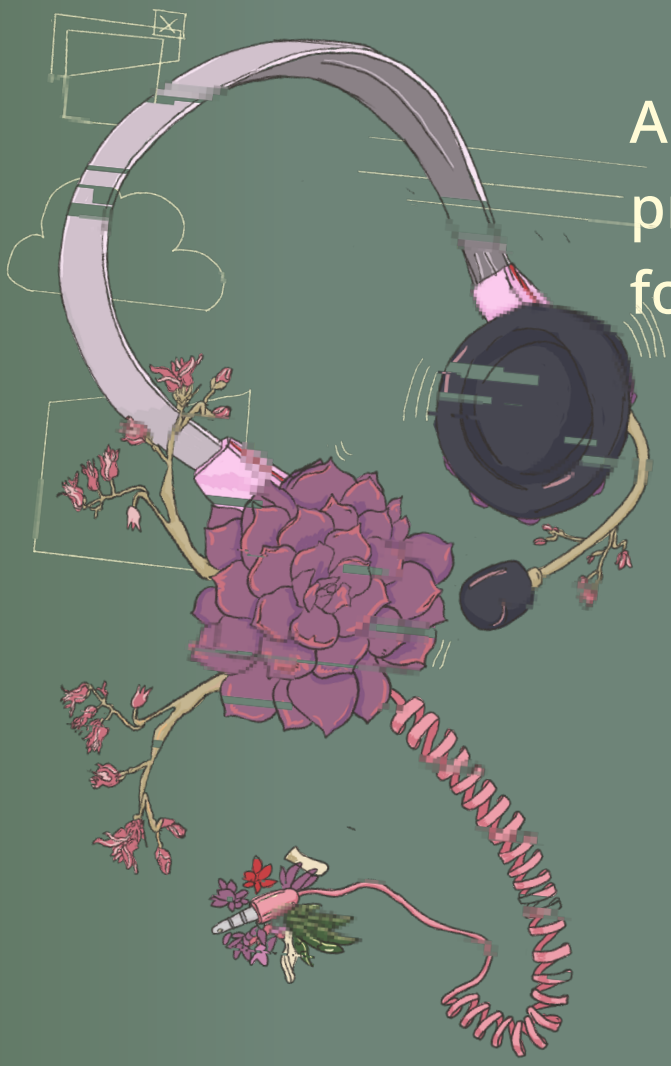


Tech Care

A step-by-step guide to providing digital support for civil society



Credits and licence

Coordinator and co-editor:
Flo Pagano, Digital Defenders Partnership

Co-editor:
Inés Binder, Digital Defenders Partnership

Copy-editing:
David E. Selden

Cover and layout:
Constanza Figueroa

Contributors:
Daniel Bedoya Arroyo, Access Now Digital Security Helpline
Inés Binder, Digital Defenders Partnership
Jean-Marc Bourguignon, Nothing2Hide
Michael Carbone, Access Now Digital Security Helpline
Mohamed Chennoufi, Access Now Digital Security Helpline
Farhanah, Digital Defenders Partnership
Alexandra Haché, Digital Defenders Partnership
Maggie Haughey, Access Now Digital Security Helpline
Rogelio López, Access Now Digital Security Helpline
Beatrice Martini, Access Now Digital Security Helpline
Etienne Maynier, Amnesty Tech
Daniel Ó Cluanaigh, Digital Defenders Partnership
Lu Ortiz, Vita Activa
Flo Pagano, Digital Defenders Partnership
Grégoire Pouget, Nothing2Hide
Hassen Selmi, Access Now Digital Security Helpline

Tech Care

A step-by-step guide to providing digital support for civil society

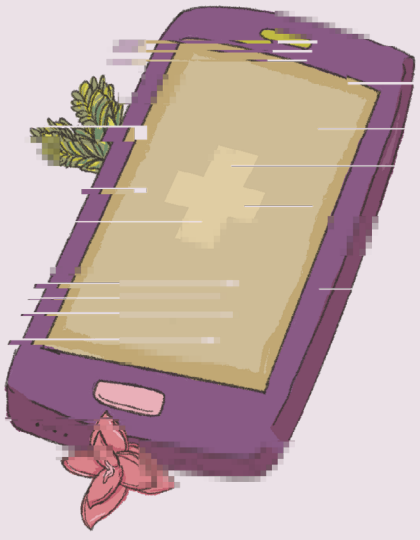
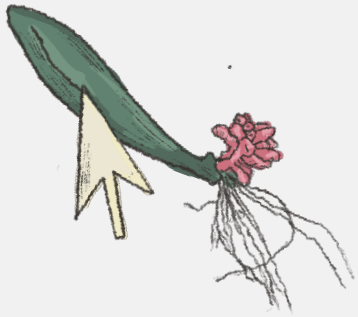


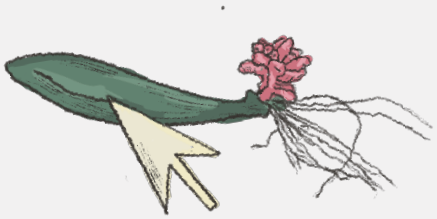
Table of Contents

Introduction



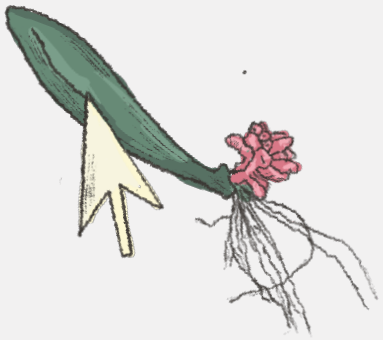
Groups that offer digital safety support to civil society have multiplied in the last decade, as activists and human rights defenders, journalists, LGBTQIA+ organisations and other minorities under attack have started to see how ICT is becoming a crucial tool for their activities, while also a powerful weapon their adversaries could use to undermine their efforts, threatening them and their allies.

A decade has passed since the first half of the 2010s when some radical technology collectives began to offer technical support to activists and international organisations, launching projects which provided digital security consultancy and training to civil society groups and human rights defenders.



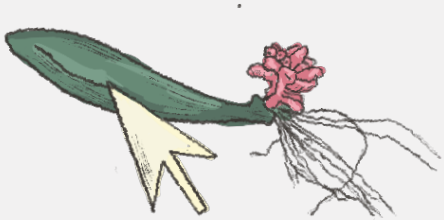
In 10 years those efforts have increased manifold, with digital security help desks being founded by small and large groups alike in every region of the planet and for the most diverse communities: journalists and human rights defenders, international organisations and grassroots movements, LGBTQIA+ groups, women's shelters and so on.

In 2015 these help desks also started networking in a more systematic way with the foundation of CiviCERT. Since then this federation of help desks and infrastructure providers for civil society has grown from the initial 5 founders to over 30 members, including local and international organisations, as well as some individuals who offer digital safety assistance in their country or region.



Still, as digital attacks on civil society and vulnerable minorities increase both in number and intensity, new digital security help desks are being created all over the world - not only for civil society and movements for social and political change, but also to better protect women, LGBTQIA+ people and other groups targeted by ICT-enabled violence and private surveillance.

This is why in the last few years CiviCERT members have received several requests to support the creation of new non-profit help desks. In some cases, it was possible to join forces among established computer emergency response teams and infrastructure providers for civil society and offer guidance, training and infrastructure to the newly-founded help desk. In other cases, when just initial orientation was needed, it became clear that the available documentation - created either for commercial and governmental Computer Security Incident Response Teams that had no familiarity with the context of civil society or for humanitarian hotlines that had no experience with digital security emergencies - did not match the actual needs of a help desk offering digital safety support to civil society groups.



What we lacked was a set of simple instructions that could help navigate the workflows and procedures of a digital security helpline, while focusing on the specific demand of offering a service to groups that are often underfunded, understaffed, non-hierarchical and exposed to disproportionate threats and the consequent risk of post-traumatic stress disorder among their staff or volunteers.

In publishing this guide we aim to fill this gap, enabling smaller organisations and grassroots groups to set up a team to respond to the digital safety needs of the people they work and fight with. It can be read by techies who want to organise and join forces to help their movement, but also by managers and organisers, who can follow the steps outlined in the initial chapters to start planning the creation of a digital security help desk for civil society and then look for people with a technical background to staff their help desk during the implementation phase.

Following the best practices established among computer emergency response teams, the first chapter of this guide describes how to decide what your help desk or helpline is going to do, for whom, and which policies will be required to deliver these services.

Chapter 2 outlines the various steps needed to make a realistic plan for your DSHCS - from getting funded to creating a secure office, up to providing the necessary infrastructure and creating and empowering your team.

Chapter 3 illustrates the most important service of your team, incident handling, from preparation to detection and analysis, all the way to containment, eradication and recovery as well as post-incident activity, including best practices on the documentation of workflows and procedures.

Finally, *Chapter 4* goes beyond the day-to-day operations of your own help desk or helpline and offers recommendations on how and why to collaborate with other digital security help desks and computer emergency teams, and on how to review your work to make sure you deliver excellent service to your beneficiaries.

We have also included a series of templates you can use to create a framework and the necessary policies for your DSHCS.

This guide would not have been possible without the existence of CiviCERT and the contributions of many of its members, who shared their documentation, drafted new content, offered interviews and reviewed the final outcome.

We would like to thank in particular:

* **Access Now Helpline** for the strong support they have offered to the creation of this guide, for generously sharing their public and confidential documentation with the curators and for organising an internal write sprint to offer great advice on how to manage a DSHCS. Many thanks in particular to: Michael Carbone, Maggie Haughey, Mohamed Chennoufi, Rogelio López, Daniel Bedoya Arroyo and Beatrice Martini. Particular acknowledgment goes to Hassen Selmi, Access Now Helpline's Incident Response Coordinator, for his interview which was the basis of the section on the Incident Handling Process (Chapter 3).
* Daniel Ó Cluanaigh, who helped tell the story of the Digital Defenders Partnership's Fieldbuilding project for community capacity building.
* Etienne Maynier, who inspired many sections on information management and communications with beneficiaries through his interview on the publication of restricted information at **AmnestyTech**.
* Farhanah, Digital Protection Facilitator at the **Digital Defenders Partnership**, for drafting the initial version of the section on procedural documentation and gathering information for other sections.

- Grégoire Pouget and Jean-Marc Bourguignon from **Nothing2Hide** for contributing to the sections on secure communications and ticketing systems, and for the enthusiasm with which they jumped into this project as soon as they joined CiviCERT.
- **Luchadoras**, for the interview they granted us on their feminist helpline.
- Lu Ortiz, Co-Founder and Executive Director of **Vita Activa** for her interview on Vita Activa's staff-caring approach.
- Mario Felaco from **Conexo**, Alexandra Haché from the **Digital Defenders Partnership**, Jannat Fazal and Shmyla Khan from the **Digital Rights Foundation Pakistan**, Harlo Holmes from the **Freedom of the Press Foundation**, and Carlos Guerra from **Internews** for helping envision and coordinate the development of this guide.
- All the feminist helplines who joined the series of webinars **"Building feminist infrastructure: Feminist helplines for people facing gender-based violence in digital spaces"** (**https://www.digitaldefenders.org/feministhelplines/**) organised by the Digital Defenders Partnership in 2021.
- All the organisations, both members and non-members of CiviCERT, that filled in the long questionnaire we drafted to gather use cases for this guide.

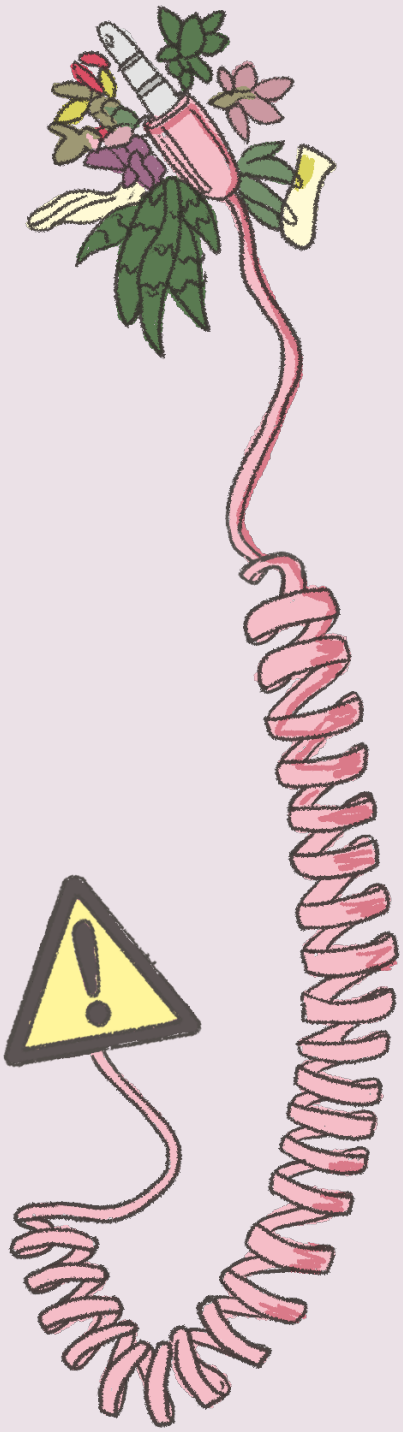
We hope this guide will support the creation of digital security help desks for civil society all over the world. Please send feedback and suggestions for improvement to: **tech-care@digitaldefenders.org**. You can also suggest improvements by creating an issue or submit a merge request on this Gitlab repository: **https://gitlab.com/rarenet/tech-care-gatsby**.

What is a Digital Security Helpline for Civil Society?

The information, support and encouragement that strangers can provide from a distance can be life-changing and sometimes even life-saving. Supporting or counselling from a distance among people who do not know each other is, in essence, an area of human action that is characterised by its diversity and heterogeneity. The reasons and motivations driving their creation and the ways those initiatives self-define and communicate about themselves can be widely different. Accordingly, the procedures, standards and policies they establish, as well as their sustainability models, can also be very diverse.

These initiatives can overlap with collective actions aimed at building networks of support and solidarity. These networks can be local, regional, national or even international, as in the case of the transnational convergence between social movements, for instance. They usually arise organically and informally from individuals and collectives that self-organise to provide solutions, services, care and attention to issues they are facing. Participation within these networks is voluntary, not motivated by economic profit but by the social capital and/or well-being that derives from citizen participation or volunteering activities.

We can interpret many of these initiatives as a self-organised response from civil society to counteract and confront the long series of injustices and violence generated by the capitalist, patriarchal and colonialist systems we live in. Among the informal networks of support and solidarity and the formalised help desks for civil society, we can find many other models for providing support to others from a distance. This Chapter intends to introduce those different models, their definitions, main advantages and characteristics.



Advantages and values of services providing support at distance

With respect to helplines in general, there are different classifications and values associated with the audiences they serve and how support should be provided. For example, some helplines are defined as "Volunteer Emotional Support Helplines" (**VESH**)[1]. They form an international network that combines the various telephone counselling services operated by three international projects - Befrienders/Samaritans, IFOTES and Lifeline.

Together, they represent 1200 member centres distributed in 61 countries. They work together to promote best practices and communication skills that contribute to emotional health, increase information sharing among participating associations and represent the experiences of their members internationally.

Complementarily, the International Federation of Telephone Emergency Services (**IFOTES**)[2] develops international standards for these listening services, which must consist of the implementation and respect of the following elements:

- Emergency Telephone Services are available, at any time, to anyone who wishes to contact, regardless of age, sex, religion or nationality.
- All callers have the right to be heard and treated with respect regardless of their beliefs, convictions and personal choices.
- Listening is offered in a welcoming and open attitude, and the listener's golden rule is never to impose any obligation on the caller.
- The content of a call is highly confidential, especially with regard to any information concerning private life.
- During a telephone conversation, the listener must remain strictly anonymous and the caller has the right to remain anonymous if they wish to do so.
- The branches work on a voluntary basis. The call handlers have been selected, trained and supervised in order to constantly improve their listening skills.
- Emergency Telephone Services are completely free of charge to the caller.

On the other hand, the **USAID manual on how to create a hotline** (Stratten & Ainslie, 2003)[3] highlights the following advantages when considering creating a new one:

- Hotlines offer an effective way to provide callers with accurate information, advice and referrals to appropriate community services or resources. The anonymity of a hotline is a key advantage, especially when working with adolescents because it allows the caller to ask questions that may be difficult or uncomfortable to address in a face-to-face setting.
- Hotlines can be a useful barometer for measuring the impact of public education and media campaigns, and can provide information to guide new interventions.
- Hotlines reinforce prevention messages disseminated through other channels, especially the mass media. Unlike mass communication, hotlines reinforce messages in an interpersonal way with person-to-person contact through telephone lines. It is this interpersonal communication that can serve as the basis for people to adopt new behaviours.

1 https://en.wikipedia.org/wiki/Volunteer_Emotional_Support_Helplines

2 https://www.ifotes.org/en/about

3 https://pdf.usaid.gov/pdf_docs/PNACU541.pdf

Traditionally, the vast majority of helplines could be contacted by telephone, and nowadays they are often complemented with other channels such as contact forms, emails, chats via instant messaging services, SMS and even bots. Each type of medium has advantages and disadvantages with respect to the kind and quality of interaction as well as the care and support it can provide.

As seen in this introduction, helplines, hotlines and help desks can be efficient services to provide accurate and timely information to vulnerable or at-risk populations, offer an opportunity for dialogue and a better understanding of what these populations feel, experience and need.

Hotlines, Helplines and Help Desks

A **hotline**[4] is a phone that automatically directs you to a pre-selected destination number. However, the colloquial use of the term "hotline" usually refers to a call centre that can be reached by dialling a specific telephone number. There are toll-free numbers for reporting crimes, calling the police, fire departments and other emergency services. These hotlines are generally managed, supported and/or financed by public institutions.

Within civil society there are crisis hotlines and helplines to prevent suicide, to support people facing violence and various forms of discrimination, to report crimes or to provide support immediately after a natural or human catastrophe (war, terrorism). Helplines can offer access to general information, specialised advice, personalised accompaniment or a more generic emotional listening and support service. These services may or may not be free of charge, may be temporary or permanent services, may be run by local non-profit organisations or by NGOs and entities working on international cooperation issues. Some hotlines or helplines may be staffed 24 hours a day, seven days a week, others may have more limited hours.

It should be noted that the terms "hotline" and "helpline" are often used interchangeably. However, it is important to emphasise that in some cases they do stand out as having clearly differentiated objectives.

Sometimes the concept of "hotline" is more oriented to temporary lines to alleviate crisis situations related to natural or human catastrophes and tends to overlap in these cases with the concept of "crisis lines". In this sense, we also see that the hotline concept tends to be used more in the context of NGOs and development cooperation. In other cases we have identified initiatives that use both concepts to differentiate between the services they offer to their constituents. For instance, SaferNet, a project founded in 2005 in Brazil, is clearly divided between the **hotline**[5] that serves to report Internet crimes and the **helpline**[6] that provides support to people facing violence on the Internet.

Besides these examples we find the concept of "**help desks**"[7], which are defined as a "resource intended to provide the customer or end user with information and support related to a company's or institution's products and services. The purpose of a help desk is usually to troubleshoot problems or provide guidance about products such as computers, electronic equipment, food, apparel, or software". Help desks are focused on providing answers and solutions to callers regarding problems or emergencies they may be experiencing with respect to their use and interaction with Information and

4 https://en.wikipedia.org/wiki/Hotline

5 https://new.safernet.org.br/denuncie

6 https://new.safernet.org.br/helpline

7 https://en.wikipedia.org/wiki/Help_desk

Communication Technologies, encompassing electronic devices, software, hardware, IT infrastructure, administration of networks, social media platforms, etc.

We find the concept of "Digital Security Help Desks for Civil Society", which typically consist of projects that provide support to activists, human rights defenders (HRDs) and/or civil society organisations facing digital risks, attacks and emergencies, to be of central interest to this guide. It is difficult to trace their origins precisely but we can name some initiatives that we feel are part of their trajectory.

For instance hacklabs, which are "rooms or buildings where people interested in technology can come together to socialise, create and share knowledge, and work on projects individually or as a team" (**Maxigas, 2014**)[8]. Hacklabs are run by hackers for hackers, where people interested in hacking ICTs (Information and Communication Technologies), developing free technologies and discussing the political implications of technologies can gather and recognize themselves. These spaces enable hacker communities to flourish and put their technical skills and knowledge at the service of other social movements and collectives, in particular when setting up autonomous IT infrastructure, learning to use it in more secure ways and facilitating the use of ICTs to inform, communicate and document their struggles.

Some examples of hacker movements that have provided remote support to other movements can be found in the hacktivist collective **Telecomix**[9], who provided support to Egyptian activists about how to circumvent state censorship of the internet using landlines, or the cyberfeminist collectives that have provided support to other feminist collectives in mitigating and overcoming gender-based violence and migrating to more secure tech infrastructure.

The multiplication of digital attacks targeting activists, defenders and civil society organisations to hinder or impede their work has been a growing trend over the last decade and has led to the emergence of more initiatives focused on setting up digital security help desks. For instance, **Access Now Digital Security Helpline**[10], which was created in 2014, is one of the first of its kind to orient its services explicitly at civil society.

As we can see, the origins of digital security help desks oriented at civil society can be linked to informal initiatives such as hacklabs and hacktivists movements which are based on distributed networks with a loose membership affiliation.

Nonetheless, digital security help desks oriented at civil society are generally based on formal rules and policies that define how they provide support to others, document their work and share sensitive information with others.

To understand this level of formalisation, we need to introduce the concept of Computer Emergency Response Team (CERT).

CERT, CSIRT and SOC

A Computer Emergency Response Team (**CERT**)[11] "operates according to very specific protocols to determine how computer incidents are managed and documented, how mitigation, warning and follow-up actions are coordinated with other entities or organisations, and what guidelines must be followed in order to share information (almost always of a sensitive and confidential nature) with other individuals and organisations".

8 https://www.coredem.info/rubrique48.html

9 https://en.wikipedia.org/wiki/Telecomix

10 https://www.accessnow.org/help

11 https://en.wikipedia.org/wiki/Computer_emergency_response_team

The first CERT© or CERT-CC (Computer Emergency Response Team) was created in 1988 by the Software Engineering Institute to respond to and mitigate the problems created by the **Morris computer worm**[12]. Although the term CERT was patented by the Institute, its use by other projects and initiatives is allowed. However, other terms such as CSIRT (Computer Security Incident Response Team), CIRT (Computer Incident Response Team), or SIRT (Security Incident Response Team), among others, are also used.

CERTs can be created at the level of an enterprise, a nation state, a critical infrastructure sector, or a group of organisations. National CERTs are also often referred to as National Cybersecurity Centres (NCSCs), which by law are usually assigned the role of CSIRTs, as well as providing additional services such as handling schemes to classify information within a country. CERTs typically provide a set of services ranging from information and cybersecurity incident management, to digital security oversight, vulnerability management and monitoring, and overall cybersecurity knowledge sharing management.

A final concept to detail is the Security Operations Centre (SOC) (**ENISA, 2020**)[13], which provides an incident detection service by monitoring networks and systems, and may also be responsible for incident response and management. In large enterprises, SOCs sometimes focus only on monitoring and detection services and then hand over incident management to a separate CSIRT. In smaller organisations, CSIRTs and SOCs often overlap with each other.

According to the reference manual developed by the Dutch national CERT (**FIRST, 2006**)[14], some of the advantages of setting up a CERT are the following:

- They establish a central coordination point for ICT security within your organisation.
- They systematically respond to ICT incidents and take appropriate steps.
- They help their constituency to recover quickly and efficiently from security incidents and minimise loss or theft of information and disruption of services.
- They use information gained during incident handling to better prepare for handling future incidents and to provide better protection for systems and data.
- They deal properly with legal issues that may arise during incidents.
- They endeavour to exchange knowledge within their constituency.

International networks such as **FIRST**[15] and **Trusted Introducer**[16] bring together various computer security incident response teams in government, commercial or educational organisations. The aim of these networks is to foster cooperation and coordination in incident prevention, facilitate rapid reaction and promote information sharing among members and the community at large. They also create standards and protocols to ensure the proper certification of CERTs.

Even if CERTs have historically tended to focus on the objectives of large companies, universities and even entire countries, their *modus operandi* can also serve the needs of civil society members such as human rights defenders, activists, non-profit organisations and citizens in general, who are the growing target of attacks and emergencies taking place in digital spaces.

12 https://en.wikipedia.org/wiki/Morris_worm

13 https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

14 https://www.first.org/resources/guides/cert-in-a-box.zip

15 https://www.first.org/

16 https://www.trusted-introducer.org/

CiviCERT

The Civil Society Computer Incident Response Center (**CiviCERT**)[17] was created in 2015. In 2016, CiviCERT became an official member of the Trusted Introducer network, a necessary step to being recognized as a CERT. Individual CiviCERT members are also members of FIRST. These accreditations provide a unique platform for presenting important digital security issues affecting civil society to a wide range of CERTs serving government and corporate entities.

CiviCERT's **membership policy and code of conduct, as well as the data and information management and vetting policies**[18] were designed to best suit the realities of the individuals and organisations that would join this project. As of 2022, Civi-CERT counted 30 organisations and three individuals. About half of its members consist of international organisations such as Access Now, Amnesty International Security Lab, Digital Defenders Partnership, Freedom of the Press Foundation, Front Line Defenders, Human Rights Watch, Internews and the Organised Crime and Corruption Reporting Project, which all do extensive work globally regarding monitoring, research, advocacy about human rights violations and digital rights and, in some cases, also provide funding, rapid response and digital security accompaniment and training.

The other half consists of smaller projects that operate in a country or at a regional level and provide rapid response, either as a help desk, or providing training and accompaniment, and/or analysis and documentation of malware and other digital threats. Among the countries represented, we can find Armenia, Brazil, Colombia, Luxembourg, Myanmar, Nigeria, Pakistan, Serbia, Taiwan, Tibet, Uganda, Ukraine and the USA, for example.

CiviCERT members share with each other updates on the rapid response cases they carry out, what kind of new risks or threats civil society actors are facing, and what resources, research or tools are being developed. Altogether these updates provide a snapshot of the global picture of digital attacks on HRDs and civil society.

In addition, support is sought in terms of knowledge or access to resources. When possible, webinars are organised to present specific cases or methodologies. Finally, CiviCERT members coordinate through a private and encrypted mailing list, and gather in face-to-face meetings either during international conferences on digital security for civil society, or through training events oriented to its members. All members have access to a range of resources and shared technical infrastructure.

For instance, CiviCERT organisations that wish to do so can be listed as a supporting organisation in the **Digital First Aid Kit**[19], a free resource to help first responders, digital security trainers and activists with technical interests better protect themselves and their communities against the most common types of digital emergencies. This resource acts as the intake mechanism for support requests to CiviCERT through a choose-your-own-adventure approach that guides the visitor through several questions to understand what their issue is and which CiviCERT member can best address their emergency. The website, which can also be used offline, is available in Arabic, Albanian, Burmese, English, French, Indonesian, Portuguese, Russian, Spanish and Thai.

17 https://civicert.org

18 https://www.civicert.org/policies/

19 https://digitalfirstaid.org/

Moreover, CiviCERT members have access to an instance of the **Malware Information Sharing Platform (MISP)**[20], the **Phishdetect**[21] project and a **Cuckoo Sandbox**[22] instance that facilitates the forensic analysis of malware, analysing what it does, what components it affects and what connections it makes.

CiviCERT and digital security help desks for civil society are still an exception, and the current CERT/CSIRT/SOC models are not usually developed with citizens and civil society in mind. They tend to be oriented mainly towards the commercial and governmental sector, and do not have an intersectional perspective in the way they analyse the risks faced by the audiences they serve but rather tend to promote an apolitical and neutral view of technologies. This can generate serious problems since cybersecurity institutes backed by public funding only give priority to commercial entities and minors, ignoring the risks faced by women, LGBTQIA+ people and traditionally discriminated and marginalised populations, all of which are often the target of electronic fraud, cybercrime and gender violence in digital spaces that are not usually portrayed and worked on by these organisations. So the burden of counteracting these dangers, risks and violence falls on self-organised civil society, which receives limited funding and support.

20 https://www.misp-project.org/

21 https://github.com/phishdetect

22 https://cuckoosandbox.org/

Design Your Framework

By creating a framework for your Digital Security Help Desk for Civil Society (DSHCS), you will describe in detail what your help desk or helpline will do, for whom, in which setting and in cooperation with whom. This exercise will also help you understand which resources you will need to assist your beneficiaries.

You should invest enough time in designing your framework as it will lay the foundations of your help desk.

This chapter will go over how to identify your constituency, analyse your beneficiaries' needs, define your mission and setting, establish your core services, set your communication parameters and specify your policies. Digital Security Help Desks for Civil Society can be very different from each other, so each one will have a different framework but the elements described in this chapter will apply to every project.

You can use the framework template at page 69 to help you think through this stage.

Download the framework template here: **https://tech-care.civicert.org/Framework_template.pdf**.

1.1 Define Your Constituency

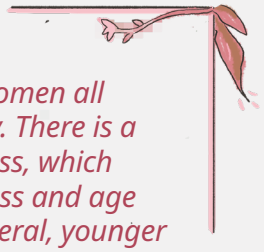
This guide will use the term "constituency" to define the whole set of beneficiaries served by a DSHCS. At the same time, a single individual or organisation will be called a "beneficiary" or "constituent".

When starting up a DSHCS it is essential to have a clear view of who your beneficiaries are and what kind of environment your services will be developed for.

Your decision on whom to serve or not to serve may be based on your organisation's mission, funders' policies, legal considerations, or even a changing political scenario that puts a specific group of people at risk.

In general terms a DSHCS's constituency is supposed to be civil society or a part of it. Still, given the broad and varied definition of "civil society" any single group can have, it may be helpful to offer a list of the kinds of beneficiaries currently being served by the DSHCSs that are members of CiviCERT:

- Activists
- Non-governmental organisations
- Human rights defenders
- Human rights organisations at risk
- Independent media
- Indigenous organisations
- Journalists
- Land defenders
- LGBTQIA+ groups
- Women
- Youth



We work with women all over the country. There is a problem of access, which is basically a class and age problem. In general, younger and middle-class women don't write to us much because they manage to solve their own problems of gender violence enabled by ICT. Then, there are older adults, children and adolescents from rural areas who are just starting their relationship with ICT. We also support people with a public profile that are constantly being assaulted. We need specific strategies for them as well. So, there is a difference between the way we are working and confronting violence with these groups.

SOS Digital (Haché, 2021).

1.2 Analyse Your Constituency's Needs

Identifying and evaluating the needs and expectations of your constituency and the context they operate in will be essential for the success of your project.

You should talk with your constituency about the real value your DSHCS could bring, analysing the threats your beneficiaries could face and their needs in response to digital security incidents and the prevention of threats. This could be done in-person or remotely, in groups or in one-on-one interviews, both publicly or privately.

There are a number of frameworks that can be used for this kind of analysis. The two most commonly used are:

- **SWOT:** to identify the strengths, weaknesses, opportunities and threats.
- **PESTLE:** to incorporate political, economic, social, technological, legal and environmental dimensions in the contextual analysis.

After analysing your constituency's needs, a good practice is to carry out a threat modelling activity to characterise the political context you will be operating in, identify the help desk's vulnerabilities and threats, together with their likelihood, and

specify the requirements for prevention and mitigation. This threat model must be taken into consideration when developing your help desk policies, technical procedures, documentation and training staff.

You will find some keys to conducting these analyses in the framework template at page 69.

Download the framework template here: **https://tech-care.civicert.org/Framework_template.pdf**

Learn more

Higson Smith, Craig, Ó Cluanaigh, Daniel, Ravi, Ali G., Steudtner, Peter (2016). Overall Framework for Context Analysis. *Holistic Security - A Strategy Manual for Human Rights Defenders*. Tactical Technology Collective. **https://holistic-security.tacticaltech.org/chapters/explore/2-1-overall-framework-for-context-analysis.html**

Front Line Defenders (2011). Understanding Your Context. *Workbook on Security: Practical Steps for Human Rights Defenders at Risk*, pp. 61-7. **https://www.frontlinedefenders.org/en/workbook-security**

Schulte, Jennifer (2018). Gender-Based Risk Model. *Cyberwomen: Holistic Digital Security Training Curriculum for Women Human Rights Defenders*. Institute For War And Peace Reporting. **https://iwpr.net/global-voices/print-publications/cyberwomen-holistic-digital-security-training-curriculum-women**.

1.3 Define Your Mission

After analysing your constituency's needs and context, your next planning step should be the drafting of a mission statement. By defining your mission you will clearly explain the purpose and function of your DSHCS and provide a brief overview of the core goals and objectives of your project.

As this will be the foundation of your work for some years it is good practice to avoid ambiguity by making the mission statement compact but not too short.

Here are two examples of mission statements by CiviCERT members:

We were producing knowledge about how women were experiencing violence in Mexico to identify it and characterize it. As part of this job, we worked to make this violence visible in the public sphere. Because of this, we became a reference, and support requests quickly began to arrive. The possibility of having a space to support women facing this violence then came up. So in March 2020, we decided to make the arrangements to accompany women asking for support and information.

Luchadoras (Haché, 2021).

Access Now Digital Security Helpline

Access Now defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

Access Now's Digital Security Helpline provides technology solutions and real-time advice for users at risk in circumstances where communications are not open, free, or safe. Through our 24/7/365 Digital Security Helpline, we offer technical guidance and incident response to inform and support activists, journalists, human rights defenders, and civil society actors on the ground.

The core goals and objectives of Access Now Digital Security Helpline are:

* To provide direct technical support to users and organisations at risk so as to identify and address their digital security needs.
* To provide assistance to users and organisations at risk to secure their digital assets, communications and other activities online, and to help them circumvent censorship and obtain access to the services they need.
* To provide expertise, support and coordination to prevent and contain malware infections and to address vulnerabilities in systems and software.
* To update our constituency about any newly-emerged threats and vulnerabilities that need to be urgently addressed.
* To coordinate support to users at risk in case this support can be better provided by other CERTs.
* To become a recognised centre of information security excellence for national and international organisations to refer to.

We challenge and disrupt the surveillance industry and the targeting of activists through digital security support, research, advocacy and campaigning. At Amnesty, each team has to define the problem they want to tackle and create a strategy of change. So we ask ourselves: "How do we change this?". This question leads to many discussions, so we focus more on research. While Access Now and other organisations provide digital support to a broad public, we do so mainly for people who are or have been targeted by surveillance. We both conduct research and digital security support.

Etienne Maynier, Amnesty Tech (Interview, December 2021).

Mnemonic

Mnemonic works globally to help human rights defenders effectively use digital documentation of human rights violations and international crimes to support advocacy, justice and accountability.

We aim to:

* Archive digital information to ensure that potential evidence is not lost and remains accessible and usable for future accountability mechanisms.
* Train human rights defenders to maximise the impact of digital information and empower those working with it.
* Reduce the impact of harmful content moderation policies by social media companies and governments by providing comprehensive, reliable data surrounding the takedowns of human rights documentation on social media platforms.
* Build and support the development of open source tools and methods to increase human rights defenders' capacity to use digital information to advance social justice.

1.4 Define Your Setting

When you plan for the creation of a DSHCS, you will need to make decisions on your organisational structure: will you be part of a larger organisation, or will you

be independently run? Will you need to fundraise on your own, or will a fundraising department provide you with resources?

Your DSHCS may adopt different organisational structures. Many DSHCSs are projects of larger non-profit organisations or work within Internet Service Providers for civil society. Others are independent and some are volunteer-based. It is also possible for multiple incident handling capabilities to exist within a single parent organisation, e.g. with one department serving the organisation's staff and addressing incidents on its infrastructure, while another serves an external constituency. Some national CERTs can include among their services handling digital security incidents that affect non-profit organisations.

The helpline acts as a referral. We refer our cases to social media platforms when needed, as we have direct communication with Facebook and their Not Without My Consent pilot. We also refer to the Internet Watch Foundation's online pilot for online child pornography and escalate removal petitions to get harmful content taken down. Sometimes we support complainants filing a complaint with law enforcement in Pakistan. Or we link women and young girls wanting to get out of toxic families or abusive relationships with shelters in Pakistan. All of this goes beyond the digital security services and the legal assistance that the helpline provides.

Digital Rights Foundation (Haché, 2021).

1.5 Define Your Core Services

A DSHCS can offer many different services but as long as you provide some kind of digital security incident response you don't need to do everything and can focus on a small set of core services, for example, focusing on the security of social media accounts or on giving recommendations on how to circumvent censorship in a specific area.

Many DSHCSs provide both reactive services - i.e. response to digital security incidents - and preventative services - i.e. digital security education efforts to reduce the risk of incidents - but in most cases they will limit their list of services based on their capacity and will decide to refer to other teams for additional services.

What follows is a list of both reactive and preventative services offered by CiviCERT members, including services that are outside of the scope of digital security:

Reactive	**Preventative**	**Not strictly related to digital security**
· Initial triage · 24/7 digital support · Equipment replacement · Handling vulnerabilities and malware · Handling account hacking · Online harassment mitigation · Forensic analysis · Censorship circumvention	· In-person training · Organisational security consultancies · Secure website hosting · Website protection · Denial of service protection · Assessing threats and risks · Securing communications · Device security · Web browsing security · Account security	· Grants and funding · Relocation of individuals at risk · Physical security · Legal support · Psychosocial support · Public advocacy

1.6 Communicating with your Constituency

Defining the ways in which the DSHCS will establish communication with its constituency is a crucial element of this framework.

You will have to decide how your constituency will get in touch, your availability and response time, and be confident about how to communicate with people who might be emotionally traumatised.

Decide How Your Constituency Can Get inTouch

You will need to identify the best communication channels for your beneficiaries to get support from the helpline or help desk.

Among the things you will need to consider, based on the initial context analysis and threat model, is whether your beneficiaries may need end-to-end encryption or an anonymous intake mechanism to start with. If this is the case, think about all the possible methods to exchange any sensitive information through a secure channel.

We recommend setting up at least two different ways to reach out to your help desk:

- A channel accessible to everyone without any technical knowledge, such as an email address.
- A secure channel for people who have the necessary technical knowledge to use it, such as an encrypted email or a secure messaging app such as **Signal** (**https://signal.org/**) or **Wire** (**https://wire.com/**).

Ensuring the safety of communications is important. However, your priority is to ensure that your DSHCS is easily reachable. For this reason, it is important to offer several communication channels for your beneficiaries. Multiplying the communication channels is not necessarily a problem as long as your team is organised enough to share information.

Here is a list of all the communications tools offered by CiviCERT members to their beneficiaries as possible methods to establish first contact with their DSHCS:

- Anonymous web form
- Email
- PGP-encrypted email
- Phone
- Snail mail
- Signal
- Skype
- Telegram
- Web form
- WhatsApp

We are operating a helpline to attend to women who are experiencing digital violence in Mexico. This initiative came about from an increase in the requests for support on our social media outlets. The main services we offer are: providing comprehensive accompaniment; psychological first aid; detecting needs; providing information such as alternatives for action, forms of reporting, content on digital violence, digital security, or contacts of possible support networks; escalation of cases through reports on various platforms; channelling to specialized organisations and institutions for optimal support and monitoring.
We have an email, a telephone line and WhatsApp. People also contact us through our social media and our website contact form. Also, through referrals from other organisations that receive cases and ask us for support.

Luchadoras (Haché, 2021).

Also consider that some of your beneficiaries might have gone through traumatic events and may need active listening and empathy, which is best achieved through a phone or video call.

There are also plenty of choices to maintain the relationship with beneficiaries and receive feedback, including:

- Forums
- Mailing lists and other community spaces
- Meetings, conferences, workshops, presentations (in-person and remote)
- Newsletters
- Social media

Declare Your Availability and Response Time

You should clearly communicate your response times to your beneficiaries to avoid false expectations and to establish an adequate Service Level Agreement (SLA) with your constituency. Giving timely feedback to beneficiaries during incident handling is crucial, both for addressing the issue they are facing and for your DSHCS's reputation.

The availability and response time of your DSHCS will largely depend on the number of your staff members and on their working hours.

Unless your DSHCS is available 24/7, you will need to decide how incidents can be reported outside of office hours.You could just choose to go through all incoming messages on the next working day, or you could have a team member on call to monitor incoming requests and decide on their urgency.

It is important to consider your context when making this decision: for example, if you have limited funding you may not be able to pay an operator for working outside standard working hours. These are important considerations for the psychosocial security of your staff as well: if, for example, your DSHCS is operated by volunteers, they may be willing to accept requests at any hour of the day or night, but this could quickly lead to a burnout of your most dedicated operators.

In terms of communication, the main thing for us is to put their needs at the centre, seeking to deactivate guilt and embracing their feelings, avoiding re-victimisation. Communication from Luchadoras is designed to make them feel as if they were a friend who responds, accepting and agreeing with the decision they make about the situation they are going through.

Luchadoras (Interview, January 2022).

Learn more

For a deeper insight on how to care for the DSHCS team's well-being, read the section on Staff Welfare Policies at page 45 in **Chapter 2**.

Define the Tone and Protocols for the Conversation

Besides ensuring that communications with beneficiaries are confidential, when responding to support requests DSHCSs should always keep in mind that their beneficiaries can be emotionally traumatised by the attack they've been exposed to.

Here are some tips on how to establish communication with a person who has faced an attack:

We brought the concepts of emotional and empathic support into our helpline. Our psychological first aid is based on three questions: "How are you doing with this stress?" to share our deep concern for their well-being; "Can you explain the problem to me?" to let them control their narrative; and "What do you want us to do for you? What is your desire?" to build solutions along with the person looking for support.

Vita Activa (Haché, 2021).

We try to publish as much data as possible: indicators, methodology, etc. For instance, with Pegasus, we also published detailed forensic traces. The more we publish, the more other people can build their own research on, but also the less we are pressured into giving more data, from governments, for example. We are then publishing detailed technical reports, so if a government comes to us, we can say: "Hey, everything is already public". That's one of Amnesty's policies: publishing evidence so that we're less prone to be asked to provide private information.

Etienne Maynier, Amnesty Tech (Interview, December 2021).

- Record the communication, check if similar communications have already been recorded.
- Use a sensitive approach, with an intersectional perspective.
- Put the requester at the centre, defusing guilt, embracing their feelings.
- Avoid re-victimisation.
- Accept and agree with the decision they make in the situation in which they are living.
- Take into account the elements of diverse contexts. Open your own eyes to cases that may come to you, without judging.

Learn more

Access Now's protocol when an incident handler feels they're dealing with a paranoid requestor: **https://communitydocs.accessnow.org/356-paranoia_protocol.html**

1.7 Define Your Policies

The policies of a DSHCS are a set of agreements and guidelines that organise its workflow and establish its standard procedures and protocols. Each DSHCS will need policies that meet its unique requirements linked to the group's mission, size, structure and services. In this section you will find a description of the basic policies DSHCSs have adopted, together with templates you can use to set up your DSHCS:

- Information Management Policy
- Incident Response Plan
- Vetting Policy
- Code of Practice
- Standard Operating Procedures (SOPs) for DSHCS Operators

After they have been developed and implemented, policies should be reviewed regularly to make sure they still apply to the DSHCS's structure, procedures, needs and capabilities over time.

Information Management Policy

Every DSHCS needs a policy on how to manage and protect information that takes into account internal operational and administrative processes

and procedures, as well as legislation and standards. It is therefore best to involve a legal consultant in the development of your information management policy.

The most basic questions to be answered in your information management policy are:

1. How is information "tagged" or "classified"?

Most DSHCSs, as well as CiviCERT, classify information based on the **Information Sharing Traffic Light Protocol (TLP - https://www.first.org/tlp/)**:

TLP:RED *Not for disclosure, restricted to participants only.* Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.	**TLP:AMBER** *Limited disclosure, restricted to participant's organisations.* Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved. Recipients may only share TLP:AMBER information with members of their own organisation, and with beneficiaries who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.
TLP:GREEN *Limited disclosure, restricted to the community.* Sources may use TLP:GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.	**TLP:WHITE** *Disclosure is not limited.* Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

2. How is information handled and secured?

You should define how you protect the information you store in your infrastructure and your communications, as well as for how long you keep information stored in your infrastructure and what happens in case of a data breach.

3. What considerations are adopted for the disclosure of information, especially if incident-related information is passed on to other teams or requested by law enforcement authorities?

4. Are there legal considerations to take into account with regard to information handling?

5. Does your policy define how your technical infrastructure and equipment should be secured and used?

You can find a template to create your own information management policy at page 83. Download the Information Management Policy template at **https://tech-care.civicert.org/Information_management_policy_template.pdf**.

Incident Response Plan

The incident management procedures described in your incident response plan are among the key measures to be put in place as they will help everyone understand what is expected of them. Describe types of incidents by distinguishing between levels of impact and establish which steps your team should follow. Define which team members should be approached if an incident arises. List the required options for scaling up or escalating matters and arrange this with your team members. In other words, ensure expectations are managed appropriately within the organisation.

In order to have a documented and coordinated approach to responding to digital security issues, your incident response plan should include the following elements:

- How cases are received and assigned
- How cases are prioritised
- the DSHCS's intake, vetting and escalation workflow
- the DSHCS's incident response lifecycle
- How cases are closed

Amnesty has a strict consent policy, so we cannot publish anything without the beneficiary's consent, even anonymously. So we have to go through a strict policy, going through the risks with them and so on. And at this point - if the case is reactive and it's not coming from a project we'd started before - we start to think about the change strategy: What do we know? What can we prove? What can we do to change this? So generally we have a discussion where we figure out what would be the advocacy plan, if there's any angle for campaigning, if there's any work that should be done with the country team, what would be the risk of publishing, what would be the benefit of publishing.

Etienne Maynier, Amnesty Tech (Interview, December 2021).

It is important for us that we have certain security protocols in place. One essential protocol is that we have everyone who works on the helpline maintain a non-disclosure agreement so that confidentiality and privacy are ensured, and that any data we keep is not personally identifiable. In this way, nobody can understand that data except the one who is handling or storing it.

Digital Rights Foundation (Haché, 2021).

You can find a template to create your own incident response plan at page 77. Download the Incident Response Plan template at **https://tech-care.civicert.org/Incident_Response_Plan_Template.pdf**.

Vetting Policy

Making sure that a DSHCS supports its real constituency is key to its reputation, so many helplines and help desks verify that requesters are really who they say they are before they start the incident handling process.

To define this verification process, it is a good practice to develop a vetting policy which describes the goals of the process, as well as the steps that operators need to take to verify the new beneficiary, get their informed consent on the process and protect their privacy as much as possible.

You can find a template to create your own vetting policy at page 89. Download the Vetting Policy template at: **https://tech-care.civicert.org/Vetting_process_template.pdf**.

Code of Practice

A Code of Practice is a document that sets out expectations for DSHCS operators with regard to how they will behave toward beneficiaries. Important elements of an effective Code of Practice include:

- Specific descriptions of common but unacceptable behaviour (sexist comments, etc.).
- Reporting instructions with contact information.
- Information about how it may be enforced.
- A clear demarcation between unacceptable behaviour (which may be reported per the reporting instructions and may have severe consequences for the perpetrator) and community guidelines such as general disagreement resolution.

Codes of Practice which lack any one of these items tend to not have the intended effect.

You can find a template to create your own code of practice at page 73. Download the Code of Practice template at: **https://tech-care.civicert.org/Code_of_practice_template.pdf**.

Other Code of Practice (also called Code of Conduct) templates and generators:

- Berlin Code of Conduct (multi language) - **https://berlincodeofconduct.org/.**
- Code of Conduct Generator based on the Contributor Covenant (multi language) - **https://github.com/sindresorhus/conduct** - based on the Contributor Covenant - **https://www.contributor-covenant.org/version/2/0/code_of_conduct** - (also multi language: **https://www.contributor-covenant.org/translations**).
- Mozilla's Diversity & Inclusion in Open Source repository, containing resources, templates and standards for making open projects more inclusive - **https://github.com/mozilla/inclusion.**

So basically we start from people coming to us for a reason. Often they come to us because they have received a weird sms or email, something like that. We then try to gather information about the context, investigate the email or the sms they've received. But first we need to make sure that they are human rights defenders, and that is quite challenging because Amnesty can have a narrow definition of what's a human rights defender sometimes, and that depends on the country team. So Amnesty International works with 2 streams: country teams and topic teams - so, like in my team: we're working on technology, but every time we work in a country we need to work with the country team. When we receive a request we have to check who the requester is and if they are a human rights defender, which is challenging because we sometimes need to ask people who they are, then we need to check with the country team whether they are human rights defenders and make sure we have approval. And then if this is the case - often with journalists, for instance, it's quite easy - we do the investigation, we try to understand what happened.

Etienne Maynier, Amnesty Tech (Interview, December 2021).

There are different good practices that we have been developing along the way. Starting with caring for the well-being of those that come to us, and also for the team. We all know that this can be exhausting, but we need to be well to accompany others best.

Tecnoresistencias (Haché, 2021).

Standard Operating Procedures for DSHCS Operators

It is important for a DSHCS to have Standard Operating Procedures (SOPs), to define, for example, how operators should respond to requests, communicate with beneficiaries, ensure confidentiality and make referrals, but also to make sure they know how to behave in stressing situations and how to cope with stress.

Learn more

Access Now Digital Security Helpline Public Documentation includes a section on their standard operating procedures:
https://communitydocs.accessnow.org/tag_helpline_procedures.html

Make a Realistic Plan

After setting your DSHCS's framework it is time to establish a general plan which outlines how to carry it out; that is, to define its material aspects. This plan should include drafting a budget to cover all your operative needs: from staff, hardware and software to renting an office if needed.

It is essential to establish how you will raise the resources to cover this budget. Will you accept funds from governmental and private actors? Will you crowd-source your funds? Will you look for partnerships with public institutions? How your DSHCS achieves financial sustainability will mostly depend on the institutional setting you defined in your framework.

An important point at this stage is also defining what tooling the DSHCS will use, especially to track cases. There are many different ticketing systems with specific features, requirements and costs. You need to find the one that best suits your DSHCS's needs. In this chapter, we share a comparison of the most popular ones so that you can make an informed decision on which one to adopt.

Your plan should obviously include a strategy to secure your staff both on the digital and physical level. We have included some basic guidelines in this chapter, although we strongly recommend hiring a specialist to create a thorough security plan, especially if you have decided to create a physical office and to self-host your infrastructure.

Finally, you should reflect on how to create and nurture your team: when planning for your DSHCS, you will need to decide what basic skills your team members need to have to provide the services you want to offer, either by hiring the right people or by training them after they've joined your team. You will also need to reflect on their roles and responsibilities and on how to care for their well-being.

2.1 Create a Budget

Based on the decisions you have made for your DSHCS, especially with regard to your organisational structure and response time, as well as services that you want to offer that imply additional costs (for example, offering grants to replace stolen equipment or paying training for your staff), the cost of your helpline will vary a lot.

Your initial core budget, which will be spent to create the DSHCS and start offering services, should cover at least:

1. Initial staff salaries, unless you are a completely volunteer-based help desk.
2. Hardware and software costs: work devices for staff, office equipment (if you have an office), software licences, etc.
3. Cost of online services like a website, a file-sharing platform, a ticketing system, etc.
4. Salaries or fees for legal consultants, deployment of services, etc.
5. Training for staff.
6. Office rental (if you choose to operate out of an office).

You can draft a minimum budget, which contemplates the essential items to be operationally viable, and a maximum budget, in case you get all the required resources.

This budget should be reviewed after the design phase is complete and all operational decisions have been taken.

Learn more

Read more on good practices to create a budget in ENISA (2020). "High-level roadmap and budget". In ENISA, *How to set up CSIRT and SOC - Good Practice Guide* (pp. 16-18) **https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc**.

2.2 Decide How Your DSHCS Will Get Funded

To ensure that your DSHCS can operate in the long term and become a reference point for your beneficiaries you will need to develop a reliable funding model to cover your costs.

If your DSHCS is part of a larger organisation, you can probably rely on your host organisation to think about how to cover your costs. But if you are an independent organisation, you should think of the following details:

- Where will the funds come from? Will you apply for grants, ask for donations, be funded by a consortium of organisations, or cover your costs by offering some paid services?
- Will you need to find several funding sources, or is one sufficient to guarantee your long-term operations? How secure is/are your funding sources?
- Is your funding source stable, or will it end at some point?
- Will you only look for financial resources, or will your DSHCS look to establish collaborative relationships with partner organisations and institutions?

Funding Policy

Some organisations also choose to have a funding policy to decide whether a new funding source is consistent with their missions and goals. For example, some groups decide only to receive donations to remain completely independent, while others may not accept funds that would influence their priorities.

Here are some examples of funding policies by CiviCERT members:

Access Now

The majority of our support comes from foundations and development agencies, with the rest coming from companies, courts, individuals, and civil society organizations.

To ensure the independence, and integrity of our organization, we accept support contingent upon the following non-negotiables:

- Access Now does not accept funding that places its staff, partners, supported communities, or mission at risk.
- Access Now does not accept funding that jeopardizes its relationship with its partners, stakeholders, or supported communities and networks.
- Access Now does not accept funding that compromises its organizational independence, including funding relationships that may influence its priorities, policy positions, advocacy efforts, regions of focus, or direct action work.
- Access Now does not accept funding that poses a risk to its reputation more broadly or with respect to specific programmatic areas of work.

The challenges we've encountered so far are related to sustainability because the helpline is a funded project.
So what if there's no funding? How do we maintain it? How do we manage it? And for that, we have created certain resources for people to access help. One of them is a portal of lawyers and professionals who can offer free legal services to women who are experiencing online harassment, for example.

Digital Rights Foundation (Haché, 2021).

Amnesty International

The overwhelming majority of our income comes from individuals the world over.

These personal and unaffiliated donations allow Amnesty International (AI) to maintain full independence from any and all governments, political ideologies, economic interests or religions.

We neither seek nor accept any funds for human rights research from governments or political parties and we accept support only from businesses that have been carefully vetted.

By way of ethical fundraising leading to donations from individuals, we are able to stand firm and unwavering in our defence of universal and indivisible human rights.

Learn more

Access Now Funding Policy: https://www.accessnow.org/financials/

Amnesty International Funding Policy: https://www.amnesty.org/en/about-us/how-were-run/finances-and-pay

2.3 Office and Physical Security

Whether you decide to set up a physical office or not, when creating your help desk, you should make a plan to protect your staff and volunteers, as well as your office and infrastructure, from physical attacks.

When thinking about physical security for your office, you should consider, for example:

- Protecting hardware that contains sensitive information: computers, external hard drives, servers, etc.
- Making sure nobody accesses the office without permission. For example, by installing a security camera at the entrance of your office or by creating awareness in your team on who can access their home offices and who can't.
- Protecting printers and printed documents from unauthorised access and destroying printed documents that are no longer in use.
- Securing routers and communications infrastructure.
- Reminding the team to never leave their computers unattended. And if they do, to always leave it locked.

Learn more

You can find physical security recommendations for your office or for volunteers working from their homes in **Access Now Helpline's Security PolicyTemplates**: **https://gitlab.com/AccessNowHelpline/helpline_documentation_resources/-/tree/master/templates/organisational_Security_Policies-Templates.**

Higson Smith, Craig, Ó Cluanaigh, Daniel, Ravi, Ali G., Steudtner, Peter (2016). *Holistic Security - A Strategy Manual for Human Rights Defenders*. TacticalTechnology Collective: **https://holistic-security.tacticaltech.org.**

Eguren, Enrique, y Cara, Marie (eds.) (2009). *New Protection Manual for Human Rights Defenders*. Protection International: **https://www.protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd- Edition.pdf.**

Tsunga, Arnold (ed.) (2007). *Protection Handbook for Human Rights Defenders*. Front Line, The International Foundation for the Protection of Human Rights Defenders: **https://www.frontlinedefenders.org/fr/file/1671/download?token=XHaqzSCK.**

2.4 Network Security

If your team is working in an office, they should have a dedicated network to connect to the internet, as well as to printers, physical servers and so on. A separate guest network should be created if you want to let visitors use your WiFi.

If you can, consider hiring a system administrator to manage your office network as well as your own infrastructure, if you have decided to self-host your online tools and platforms.

2.5 Infrastructure and Tooling

In theory, you can start a DSHCS with just a computer for each of your staff members and a secure collaboration platform like a self-hosted NextCloud, Gitlab, or Discourse instance to share information among team members, organise tasks, keep track of contacts and so on. You could even rely on a friendly service provider to host such a platform for you where compatible with your threat model. You can find a list of providers in Access Now Helpline's community documentation: **https://communitydocs.accessnow.org/282-Secure_file_sharing_storage.html**.

If your budget allows for it, when making plans for your digital security help desk you should consider using tools that have been created on purpose for handling incidents, identifying indicators of compromise, sharing information and analysing malware.

Many digital security help desks for civil society use the following tools to handle and analyse incidents:

- A ticketing system to manage support requests and cases (see below, section Ticketing Systems).
- A self-hosted or a federated instance of **MISP**, **https://www.misp-project.org/** for sharing, storing and correlating indicators of compromise.
- A malware analysis system like **Cuckoo Sandbox**, **https://cuckoosandbox.org**.
- Sometimes, a CRM for managing contacts like **CiviCRM**, **https://civicrm.org**.

In general, when choosing a tool or service, it's best to follow these guidelines:

- The software should be free and open source.
- Ideally, it should be self-hosted or otherwise hosted by a trusted entity.
- If the service is hosted by a third party, it should be end-to-end encrypted, audited and offer a good level of security (e.g., 2-factor authentication).

Ticketing Systems

As soon as a support request is received the person in charge of the case should start noting down every detail regarding the beneficiary, the incident and any action that has been taken to handle it. Recording all communications with the beneficiary, as well as every step taken to detect and address the incident, can facilitate collaboration with other team members and referrals to other organisations, help improve incident handling procedures and provide useful evidence that may be needed in a court of law.

Cases can be documented in many ways, even in text documents or on paper, but using a ticketing system will simplify this task as this kind of tool makes it possible to record and organise every communication and detail in a systematic way, allowing to track each support request, as well as beneficiaries and relevant third parties, and to review past cases for the sake of quality assurance and to obtain statistics, just to name a few critical features that can be helpful for a DSHCS's work.

Since communications pass through the ticketing system and are stored there, one of the essential features a DSHCS should look for when choosing the tool they will use to track requests is the possibility to secure communications and information on incidents. Therefore, it is recommended to choose a system that is compatible with encrypted communications tools such as GPG-encrypted emails or secure messaging apps like Signal.

Furthermore, a ticketing system should allow recording the following information:

- The beneficiary's name and email address.
- The beneficiary's vetting status (vetted, non vetted, rejected).
- The kind of constituency the beneficiary belongs to.
- The current status of the incident (new, open, closed, etc.).
- The urgency and priority of the incident.
- A summary of the incident.
- The kind of service requested to address the incident.
- All communications with the beneficiary.
- Evidence gathered during the incident investigation.
- Indicators related to the incident.
- Other cases related to this incident.
- Actions taken on this incident.
- Contact information for other involved parties (e.g. intermediaries, companies that have been reached out to for an escalation, partners who are helping handle the case, etc.).
- All communications with other involved parties.
- Comments by incident handlers.
- Next steps to be taken.

What follows is an overview of the ticketing systems most commonly used in the sphere of digital security support for civil society.

Zammad and CDR Link

Zammad (**https://zammad.com**) is an open source web-based help desk and customer support system with features to manage customer communications via several channels like telephone, Facebook, Twitter, chat and email, among others.

In view of the specific needs of civil society and human rights defenders, the **Center for Digital Resilience** (**https://digiresilience.org**) has developed **CDR Link** (**https://docs.digiresilience.org/link/about**), a privacy- and security-focused ticketing system based on Zammad that features custom messaging plugins for Signal, WhatsApp, and GPG, to secure communications. CDR Link requires Google accounts to log in and is hosted in AWS.

Zammad can also be integrated with NextCloud (from version 20 onwards): the **Zammad integration app for NextCloud** (**https://apps.nextcloud.com/apps/integration_zammad**) provides a dashboard widget with a Zammad ticket overview, support for finding Zammad tickets using NextCloud's unified search and notifications on status updates to tickets.

RequestTracker

Request Tracker (**https://bestpractical.com/request-tracker**), or RT, is an open source issue tracking and workflow platform developed and supported by **Best Practical Solutions** (**https://bestpractical.com**).

RT can be self-hosted, but there are also options for managed hosting or cloud hosting with AWS. It can be integrated with PGP encryption and is one of the most commonly used ticketing systems for computer emergency support teams. Among these, it's worth noting how solutions documented while handling an incident can be promptly turned into procedural documentation within RT itself - for more information see **https://rt-wiki.bestpractical.com/wiki/Articles#Extracting_an_Article.**

Freescout

Freescout (**https://freescout.net**) is a free and open source ticketing system that can be easily deployed even on shared hosting. It can be self-hosted, but **managed hosting is also available** - see **https://github.com/freescout-helpdesk/freescout/wiki/Cloud-Hosted-FreeScout.**

Freescout offers paid modules that can extend its functionalities: **https://freescout.net/modules/**, including integration with:

- PGP (only signing and encryption): **https://freescout.net/module/mail-signing**.
- WhatsApp: **https://freescout.net/module/whatsapp**.
- Telegram: **https://freescout.net/module/telegram-integration**.
- Twitter: **https://freescout.net/module/twitter/**.

Trac

Trac (**https://trac.edgewall.org**) is an open source, web-based project management and bug tracking system that can be used for tracking tasks, issues, and incidents and is sometimes used by help desks to manage their cases. It can be self-hosted but managed hosting is also available.

- Read more on how to use Trac for tracking tasks, issues, and incidents: **https://trac.edgewall.org/wiki/TracTickets**.
- Read more on managed hosting options: **https://trac.edgewall.org/wiki/CommercialServices**.

GLPI

GLPI (**https://glpi-project.org**) - a French acronym for _Gestionnaire Libre de Parc Informatique_ or "Free IT Equipment Manager"- is a free and open source tracking system and service desk system. It can be self-hosted but managed hosting is also available.

- Read the documentation on how to self-host a GLPI instance: **https://glpi-install.readthedocs.io/en/latest/**.
- Managed hosting for GLPI: **https://www.glpi-network.cloud/**.

Primero and GBVIMS

Primero (**https://www.primero.org/**) is an open source self-hosted software platform for social services case management and incident monitoring, including child protection and gender-based violence.

Based on Primero, the Gender-Based Violence Information Management System (GBVIMS - **https://www.gbvims.com**) is a data management system that enables those providing services to survivors of gender-based violence to effectively and safely collect, store, analyse and share data related to the reported incidents.

Others

There are many useful tools that can integrate the tickets of the handling process in your current workflow. As we mentioned before, if your organisation is already using NextCloud there is a specific plugin for Zammad integration: **https://apps.nextcloud.com/apps/integration_zammad**.

If your organisation is using Discourse you can add a ticketing system using the tickets and assign plugins.

- Discourse tickets plugin: **https://meta.discourse.org/t/tickets-plugin/97914.**
- Discourse assign plugin: **https://meta.discourse.org/t/discourse-assign/58044.**

A regular ticketing style tool may be overkill for small organisations. There are many project management tools that can do a great job and that are way easier to use. For instance, NextCloud Deck (**https://apps.nextcloud.com/apps/deck**) is a simple and easy way to handle tickets. Its simplicity is a great asset for small organisations. In NextCloud Desk each ticket is a task, a task has a description, is qualified with tags, has a start and a due date and can be moved from one column to another in order to replicate the ticketing workflow.

Its simplicity is a great asset for small organisations. In NextCloud Desk each ticket is a task, a task has a description, is qualified with tags, has a start and a due date and can be moved from one column to another in order to replicate the ticketing workflow.

2.6. Team Management

Any DSHCS requires a team of people with a specific set of skills to respond to support requests in a timely and accurate manner. The size and seniority of your team will depend on your organisational structure and funding situation and on your ability to create, manage and care for their professional development and well-being.

Desired Skills

A DSHCS should define the skill set needed for it to perform its mission. Since the task of your help desk is responding to digital security requests, there is a core set of skills that the team should work on fulfilling.

The following is an indicative list of technical and soft skills that members of a DSHCS team should have. If your team does not have a needed skill, you will need to identify a third party to outsource the task for which the missed skill is needed.

Technical Skill Set

- Ability to perform GNU/Linux-UNIX system administration.
- Ability to perform web server administration.
- Familiarity with the most widespread operating systems: Windows, GNU/Linux, macOS, Android and iOS.
- Ability to work with at least one network analysis tool such as Wireshark, tcpdump, Zeek, Snort, etc.
- Working knowledge of the entire TCP/IP or OSI network protocol stack, including major protocols such as IP, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol 3 (POP3), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP) and SSH.
- Working knowledge of popular cryptography algorithms and protocols such as Advanced Encryption Standard (AES), Rivest, Shamir and Adleman (RSA), Message-Digest Algorithm (5) (MD5), Secure Hash Algorithm (SHA), Kerberos, Secure Socket Layer/ Transport Layer Security (SSL/TLS) and Diffie-Hellman.
- Ability to perform vulnerability assessments and work with penetration assessment tools such as Kali Linux, Metasploit, etc.
- Scripting knowledge with languages and tools such as Python, bash, awk, sed, grep, etc.
- Familiarity with techniques and tactics of attacks.
- Solid understanding of end-user management of social media platforms like Facebook, Instagram, Twitter, Youtube, etc.
- For those working with malware reverse engineering, knowledge of assembly code in Intel x86 and work with various utilities that aid in malware analysis, such as SysInternals, as well as tool suites used to decompile and examine malware like IDA and Ghidra.

Certainly, candidates with a background in computer sciences and computer security studies would be best prepared to master these skills. However, people who are enthusiastic about such fields could earn and demonstrate these skills quickly as well. When hiring, you should assess studies, experience and level of enthusiasm to identify the right candidate to join your team.

Usually, while a help desk is being created, it is not always possible to have these skills as quickly as one may want.

Management should therefore focus on identifying the capabilities that are absolutely needed to fulfil the DSHCS's mission and then fill gaps by training team members, conducting a targeted hiring campaign, or outsourcing certain tasks to other teams.

Soft Skills

Soft skills are as important as the technical ones, especially for the handlers who will be in direct contact with beneficiaries.

- Good written and oral communication in English, to coordinate with other partners, and in the local languages of the region they will be focusing on.
- Ability to thrive in high tempo, high-stress environments.
- Strong team player.
- Ability to provide on-the-job training and knowledge sharing to other team members.
- Self-initiative with strong time management.
- Solid sense of integrity and identification with the mission of the DSHCS.
- Strong cultural understanding and experience across the region of focus.
- Broad understanding of the DSHCS constituency's political context.
- Intersectional sensitivity in approach to beneficiaries.

Roles and Responsibilities

There are many roles in a DSHCS team, each with different responsibilities. Having these in mind can help you design your team structure and identify which positions you need - or are able - to fill in according to your framework and budget.

- First-line incident handlers - These are the core members of the team. They are the ones who will be in touch directly with the beneficiaries and coordinate the multiple tasks that will lead to a successful response to the beneficiary's request. In addition to the communications skills needed to understand the beneficiary's needs and send them instructions, first-line incident handlers should be able to follow internal communications among team members, identify gaps in documentation and master the different resources that are available for them to perform incident handling such as (1) software like ticketing systems, secure communications software and tools to perform triage; and (2) human resources, whether internal, such as second level analysts, or external, such as external analysts, services providers and partners.
- Shift manager - In small help desks, this could be the director. Their role is to manage the incident handlers.
- Second level analysts - Their role is to provide technical support to incident handlers when dealing with challenging cases.
- Operations manager - They manage the finances of the team and their needs in terms of hardware, location, logistics, etc. Such tasks could be taken on by the director in small help desks, then more staff could be hired for this role, or it could be outsourced.
- Documentation coordinator - The role of the documentation coordinator is to manage the DSHCS's knowledge base. They should make sure that existing documentation is maintained and help identify gaps and opportunities to edit and create the necessary documentation for the help desk and especially for the first-line incident handlers to perform their task.
- Sys admin - Their role is to create and maintain the infrastructure that the help desk will use in their day-to-day work. The task could be outsourced or fulfilled by the director or the handlers in small help desks.

* Legal counsellor - A legal counsellor will help assess the legal security of the different interventions carried out by the help desk and make sure its policies comply with the existing legal framework (personal data protection, for instance).
* Psycho-social counsellor - A psycho-social counsellor can train DSHCS incident handlers to respond to requests for support without revictimising and develop the necessary skills for dealing with people under emotional distress.
* Outsourcing tasks - When outsourcing any task, make sure there is a high amount of trust with the team or person you are outsourcing to. Given the mission of a help desk working with civil society and human rights defenders, contracts and non-disclosure agreements are certainly necessary but not sufficient to guarantee the level of security needed by a DSHCS's constituency.

Create Your Team

Staffing your help desk operation is a crucial process for the success of the project. In addition to their technical and soft skills, your DSHCS's team members should have a strong alignment with your team values and an honest commitment to supporting your constituency. When looking for new team members, consider the following aspects:

* Trust with the communities you support is more important than purely technical skills. Alignment with values and commitment to the team's mission should be among the top requirements for all positions.
* It is always possible to develop technical skills as long as there is time and there are resources to support the development pathway.
* Onboarding processes make a big difference to how quickly members of your help desk can start providing quality assistance to beneficiaries. When possible, create written guidelines on all the topics that should be covered and follow a mentoring approach.

You can decide to hire someone and then train them on skills they need to have when working for your DSHCS, or you can launch a community capacity-building campaign to train activists who may then collaborate with your help desk. If you use this approach, it will be best to base your training sessions on a **holistic approach** (see for example the *Holistic Security Trainers' Manual* at **https://holistic-security.tacticaltech.org/trainers-manual.html**) and on a framework like the Activity-Discussion-Inputs-Deepening-Synthesis – or ADIDS – model.

Between 2019 and 2021, DDP implemented a project to build the capacities of trainers who could provide sustainable and holistic safety and security support to human rights defenders in South-East Asia, Latin America and Africa. This process took place in two phases: on the one hand, it aimed to strengthen the capacities of protection providers in general; on the other, it aimed to directly engage some of the participants to carry out accompaniment processes. When finished, DDP opened a call allowing participants to show their interest in becoming part of DDP's team of Digital Protection Facilitators. The project was a cornerstone of DDP's broader project of decentralising and strengthening the extent to which its team is embedded in, and driven by, human rights movements in the Global South.

Daniel Ó Cluanaigh, Digital Defenders Partnership.

Learn more

How to Approach Adult Learning – Level Up: **https://level-up.cc/before-an-event/levelups-approach-to-adult-learning/.**

How to Design Sessions Using ADIDS – Level Up: **https://level-up.cc/before-an-event/levelups-approach-to-adult-learning/.**

A training of trainers module on adult learning and ADIDS – Fabriders: **https://www.fabriders.net/tot-adids/**.

Training and Professional Development

In order to develop knowledge and capacity within the help desk team, different opportunities should be available as a single working strategy for everyone might not be possible or ideal.

Individual team members should work together with their direct managers to create training and development plans.

These plans should be regularly consulted, and progress should be noted as actions take place or during performance reviews.

Actions on individual action plans can vary from following online training, to acquiring books and magazines to attending in-person training.

In addition to these personal plans, the help desk organisation should continuously share resources internally, especially on subjects that are relevant to all team members, such as technical subjects on digital safety and others, including self- care, psychological support and physical security.

Provide Materials and Encourage Self-Learning

Help desk managers should circulate resources within the team to increase their technical skills on different security- related subjects. This should be an open invitation to team members to review and use those resources, but there should not be follow-ups to ensure the information is being used. The main objective is to provide the team with information that suits their interests and develop a self-learning culture throughout the team.

In addition to online resources, books and magazines that are considered appropriate and beneficial to help desk work can also be provided to the team. The magazines and books will be provided on request by team members or when the help desk management considers they can have a positive impact on the team development.

Paid External Training

When appropriate and where resources allow it, help desk management should approve participation in technical training based on the team members' individual development plans.

Conferences

You should aim to provide your team members with at least one opportunity per year to attend a help desk-related event.

You should track upcoming conferences and try to attend events that are relevant to your work with civil society groups and other organisations and individuals who provide these digital security services.

One of the best ways to find relevant conferences and events is to ask your beneficiaries what events they go to or would like your team members to attend.

Example Conferences That May Be Relevant to a Civil Society-Focused Help Desk

Event	Frequency	Website	Content
Bread&Net	*Annual*	https://www.breadandnet.org/en/	Annual unconference that promotes and defends digital rights across Arabic speaking countries
Chaos Communications Congress	*Annual*	https://events.ccc.de/	Technical knowledge acquisition, meet new beneficiaries or partners
Dublin Platform	*Every two years*	https://www.frontlinedefenders.org/en/programme/dublin- platform	Biennial gathering of human rights defenders
FIFAfrica	*Annual*	https://cipesa.org/fifafrica/	Forum on Internet Freedom in Africa
Global and regional Rapid Response Network meeting	*Annual*	https://rarenet.org	Meeting of Rapid Response Network members
Global Internet Governance Forum	*Annual*	https://www.intgovforum.org	A multistakeholder governance group for policy dialogue on issues of Internet governance
ILGAWorld (& regional conferences)	*Annual*	https://ilga.org/world-conferences	Global and regional gatherings of LGBTQIA+ changemakers
MozFest	*Annual*	https://www.mozillafestival.org/	Tech conference organised by Mozilla
Regional Internet Governance Forums	*Annual*	https://www.intgovforum.org/multilingual/content/regional-igf-initiatives	regional conferences for policy dialogue on issues of Internet governance
Global CiviCERT meeting	*Annual*	https://civicert.org	Meeting of CiviCERT members.
RightsCon	*Annual*	https://rightscon.org	Global meeting on digital rights organised by Access Now
Stockholm Internet Forum	*Annual*	https://stockholminternetforum.se/	International forum advancing a free, open, and secure internet as a driver of global development

Trusted Introducer Events

CiviCERT (**https://civicert.org**) is a CERT accredited by Trusted Introducer ( ), and as such CiviCERT members can participate in meetings and training sessions for security and incident response teams. Upcoming events are listed at: **https://www.trusted-introducer.org/events.html**.

Online Platforms

You could also provide your team with access to courses on online platforms. These courses are usually less expensive than in-person courses and allow team members to take them at their pace and as the workload allows.

Some of these platforms could be:

- **Pluralsight: https://pluralsight.com/**
- **Udemy: https://www.udemy.com/**
- **Cybrary: https://www.cybrary.it/**
- **Coursera: https://www.coursera.org/**

Skill-Sharing Sessions

Team members who gain skills that could be useful to the rest of the team either while doing their work or after undertaking training should be encouraged to document them through articles and provide skill-sharing sessions for their colleagues. If the skill-sharing sessions are recorded they will serve as learning support for the team and new hires.

Staff Welfare Policies

When working at a help desk, incident handlers deal with a wide range of distressing situations that can affect them.

Caring for your team's psycho-emotional well-being prevents burnout and increases the quality of the attention provided.

It is a good idea to care for your team's well-being as much as you do for your beneficiaries. Therefore, you should allocate all kinds of resources - time, human resources, money, etc. - to adopt a psycho-emotional care approach in your team management strategies.

There are no universal ways to achieve this. They will depend on your team's needs and their notion of care. Some caring strategies to safeguard your team's well-being are:

We prioritise a balanced workload among the caregivers.
We rotate the reception of new cases from week to week in order to distribute them equally. At the same time, it is common for there to be weeks in which the number of cases that come to us increases, and when this happens and exceeds the possibilities of the accompanier, we look for strategies to reorganise the follow-up of cases and lighten the load.

Luchadoras (Interview, January 2022).

- Even if your help desk is voluntary-based, provide good working conditions: allowance, benefits, holidays, etc.
- Allocate a percentage of your budget (up to 30%) to collective self-care activities.
- Plan short shifts to allow incident handlers to focus and provide better attention.
- Establish weekly meetings to discuss the cases and provide collective insight.
- Include the figure of a mental health advisor to support the incident handlers in avoiding burnout or stress.
- Provide a check-in instance every time an incident handler's shift begins to assess if they are in a good place to provide support. If they are not, a ringer incident handler with no specific shift assigned can replace them.
- Establish a set of parameters for when a call is too risky and requires escalation to a manager quickly. For instance, if the person calling is at imminent risk. Having these steps in mind will protect the incident handler from excessive stress.
- Plan an annual all-team meeting to discuss challenges, identify learnings and adjust the help desk's care strategies.

You can draft a staff caring policy that sets out all these strategies and to which the team and managers can refer for creating a healthy working environment. Also, consider a psycho-emotional approach when drafting your incident handling procedure - ensuring balanced triage and case assignment among the team members, for example -, code of practice, internal complaints mechanism and other policies.

Incident Handling Process

A key part of the work of many DSHCSs is incident response. Every help desk should clarify beforehand the steps and resources needed for dealing with a request for support.

The incident handling process is continuous, and generally consists of the following four stages:

Stage 1: Preparation

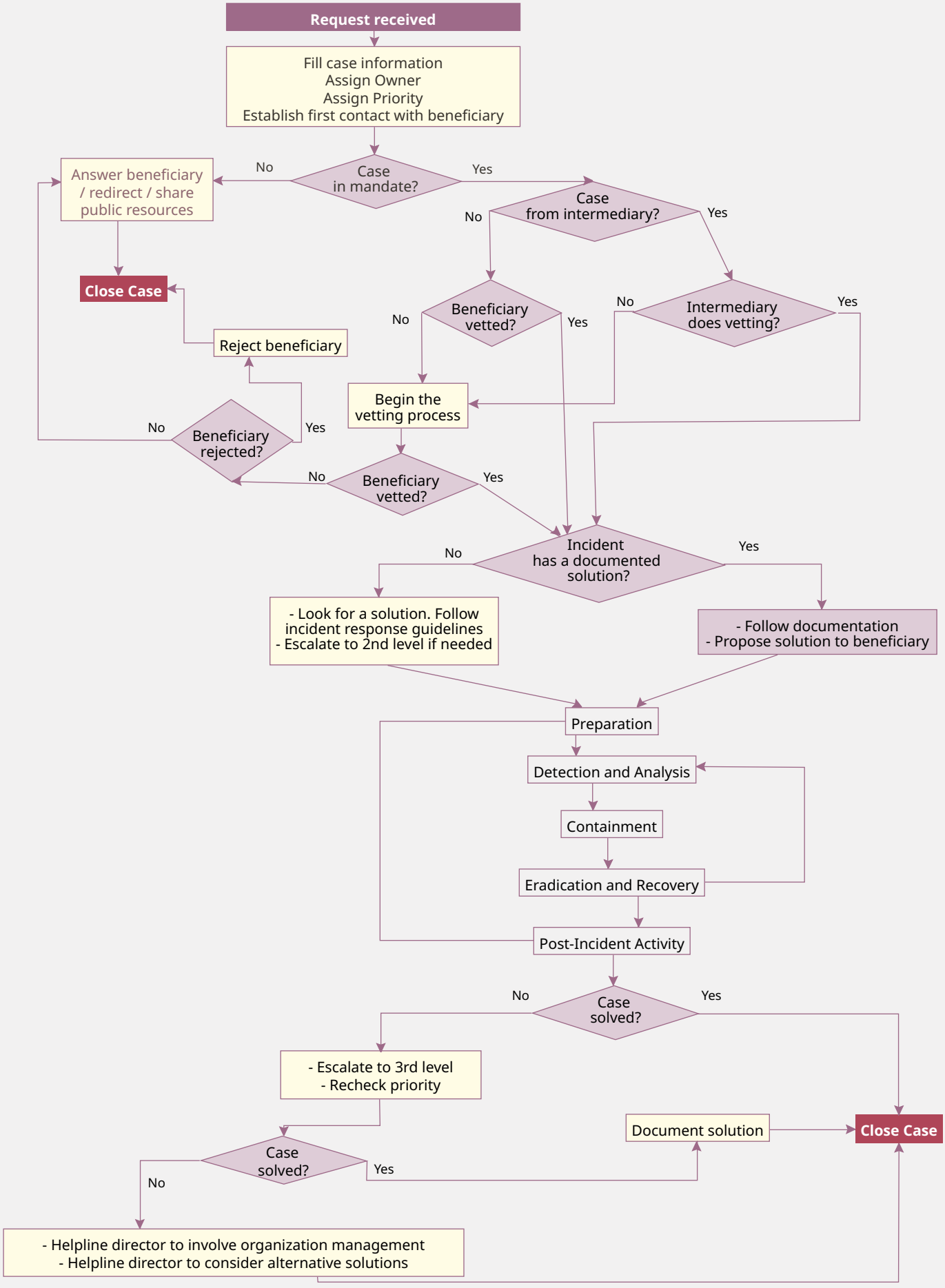
Stage 2: Detection and Analysis

Stage 3: Containment, Eradication and Recovery

Stage 4: Post-incident Activity

The incident handling process should not be limited to the containment, eradication and recovery stage: other steps should be taken, for example, in the preparation phase and post-incident activity. This process should be documented and organised so incident handlers always have each step in mind at every stage of the process and are all able to reduce the chances that the same incident may happen again.

You can see below a flowchart representing Access Now Digital Security Helpline's incident handling workflow:



The incident handling process should also be adapted to the needs and threat model of a helpline's constituency. For example, a DSHCS should consider that attacks targeting civil society are usually sophis ticated and aimed at people who are not prepared for such attacks. So a DSHCS will need to focus on the preparation and post-incident activity stages, to go beyond simple recovery and turn an incident into an opportunity to prevent similar attacks in the future.

Learn more

An example of an incident response plan is NIST (2012). *Computer Security Incident Handling Guide*. **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**. Check pages 21-44 for more information on the incident handling process.

Kral, Patrick (2021). *Incident Handler's Handbook*. SANS Institute. **https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901**.

3.1 Preparation

The incident handling process starts when a request is received: at that point the handler notes down basic information on the case, assigning it a priority and an owner and acknowledging the reception of the request to the requester. Then there is a mandatory check to make sure that both the requester is within the DSHCS's list of beneficiaries and that the requested service can be provided by the DSHCS.

We have seen a higher level of threats with a low level of security and authority: our help desks have no authority over the beneficiaries. We can recommend things, we can advise them to do things, but it's up to them if they do them or not. Most of the time they are working remotely, and it's really hard to execute exactly what we wish we could execute like other CERTs in other sectors would do, so we have to adapt this also.

Hassen Selmi, Incident Response Lead, Access Now Digital Security Helpline (Interview, November 2021).

If the request falls outside the DSHCS's mandate, the case is closed, possibly by sending the requester a list of available alternative resources. If, on the other hand, the request is within the DSHCS's mandate, vetting of the beneficiary is a recommended second preliminary step. Each DSHCS should have a vetting policy and implement it in this step, making sure that every beneficiary is who they say they are before handling their request. See Vetting Policy section in **Chapter 1**.

After checking the mandate and vetting, the incident handling process starts, but this also needs to be prepared. The preparation stage of the incident handling process also consists of creating the proper documentation that will allow handlers to promptly respond to a set of known incidents and train the staff to follow these instructions (see below, section 3.5 Documentation of Procedures, p. 51).

The preparation stage also includes outreach campaigns and training for beneficiaries who want to better secure themselves or their organisation. During this phase a help desk may also work at networking by establishing relationships with service providers or creating partnerships with other helplines and defenders to improve their capacity to escalate cases that need collaboration to be solved.

The work spent on the preparation stage will determine the speed, efficiency and quality of a DSHCS's response.

3.2 Detection and Analysis

Ideally, the incident response process starts with the preparation stage. Yet, realistically it often begins at the second stage of the incident handling process, when a request for support is received.

The first step of this stage is detection, which is aimed at making sure that what the beneficiary is observing is an actual digital security incident, i.e. that the behaviour the requester has observed is abnormal.

The incident handler should ask the requester for all the information available: system and network log files, screenshots, error messages, antivirus reports, suspicious emails, perceived symptoms of changes in normal behaviour, and other evidence that may indicate that an event is a security incident. Incident handlers should be open to any possibility and not let any digital security incident go unconsidered.

If the person asking for support is in emotional distress, gathering the necessary information to determine the incident can be revictimizing. In these cases, all the data can be gathered with the help of a person appointed by the requester.

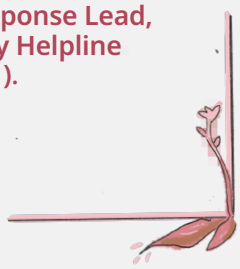
The following step in this stage is to analyse the incident to better understand what is happening and what its causes are.

The more evidence available, the better the insight the incident handler can provide.

It is very important for a DSHCS to have a common workflow that every staff member is familiar with, so we share duties and know what we do when an incident happens - how we handle it and how we work from phase to phase. This should be written, it should not be something that just happens, because that leads to some mistakes. This workflow has not only been used by us, but also by other CERTs, and it's agreed upon, and also it's framed in a way that it takes into consideration not only the kind of beneficiaries we are helping, but also our capabilities. So it helps any handler to navigate incidents from the detection to the recovery, but also to get prepared for it.

If you look at the workflow diagram, it looks like it starts when the incident starts, but in reality and in practice the preparation phase should go on continuously before any incidents happen: it is a proactive phase.

Hassen Selmi, Incident Response Lead, Access Now Digital Security Helpline (Interview, November 2021).



Different pieces of evidence may be symptomatic of the same particular incident or different ones. Making correlations between pieces of evidence in the wrong way can lead to misinterpretation of the facts. A helpful way to prevent this is to conduct the analysis collectively in regular incident discussion meetings.

A tool to start analysing some of the most common digital security issues affecting civil society is the Digital First Aid Kit, a free resource to help rapid responders to troubleshoot the most common types of digital emergencies: **https://digitalfirstaid.org**.

As in the previous stage, incident handlers should remember to record all relevant information and document every step taken.

3.3 Containment, Eradication and Recovery

Once they have confirmed that what the beneficiary is facing is a digital security incident, the incident handler will move on to the containment, eradication and recovery stage. The first step is containment - a "stopping the bleeding" interven-

tion to ensure the attacker can't have further access to the beneficiary's digital assets. The incident handler should promptly provide the instructions for containment to limit the damages quickly.

Of course, the procedure required for containment is based on the type of asset that is under attack. For more information on the various procedures, a good shared resource is **Access Now Helpline's Community Documentation**: **https://communitydocs.accessnow.org**.

Eradication is about removing anything the attacker may have added. This isn't always easy because malicious actors are usually very creative in devising new approaches for their attacks.

Afterwards, the recovery step is intended to restore the affected systems and take the necessary measures to prevent new incidents. Monitoring, therefore, becomes essential to detect any other methods an attacker can use and any further data exfiltration. Since civil society helplines often cannot monitor beneficiaries' assets directly, this step can be replaced by training the beneficiaries on how to do monitoring on their own.

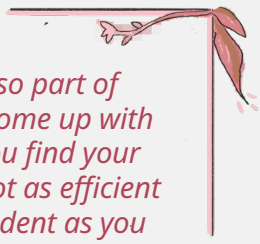
Sometimes a case can't be closed by its owner due to a lack of time or capacity. In these cases involving other members of the DSHCS team can be required to outsource the handling of the case, or part of it, especially with analysis. This is one of the situations where **networking and collaboration among DSHCSs** can be particularly helpful (see Chapter 4 for more details).

3.4 Post-Incident Activity

The last stage of the incident handling process aims to gather what the incident handler has observed when working on the case. While already known opportunities to mitigate the digital security incidents might have been identified and provided to the beneficiary, some new ways of approaching an issue might also have been found, and should be documented.

These lessons learned will improve the help desk's documentation with a more creative and accurate approach to incident handling. We recommend not to delay this documentation after the case is closed, as little details tend to be forgotten.

Sometimes an incident can be connected to a series of attacks other groups of people should be warned about, so outreach and networking with partners are often needed at this stage in order to spread public alerts describing this kind of incident to potential targets.



The last steps are also part of the process. If you come up with a new solution or you find your documentation is not as efficient to navigate that incident as you wished, as a handler you are also requested to suggest solutions based on what you have seen. Sometimes you can also suggest this before the process itself, because you realize a process will not really work so it has to be improved.

Hassen Selmi, Incident Response Lead, Access Now Digital Security Helpline (Interview, November 2021).

3.5 Documentation of Procedures

The term "documentation" is quite extensive. It may refer to several elements, and if not defined clearly, it can lead to confusion. In incident response, there are two different kinds of documentation, both as important: the documentation of cases, on the one hand, and the documentation of procedures, on the other.

The documentation of cases, which usually happens through a ticketing system (See section 2.5 Infrastructure and Tooling in Chapter 2) or other secure platforms, consists in noting down all communications with the beneficiary as well as the way a handler decided on a technical solution for solving the case, what evidence they collected, what led them to make those suggestions and what resources they consulted. This makes it possible to track down how a case was solved and, if a new solution is found, will lead to the second kind of documentation.

The second kind of documentation, which is developed during the preparation stage of the incident handling process and reviewed during the whole cycle, is the documentation of procedures. This is the technical documentation which contains strategies to troubleshoot the incidents faced by our constituency.

In the work of a DSHCS, the documentation of procedures is critical to make sure that incidents are handled correctly and quality is assured. By documenting your procedures, your team can rely on a constantly updated knowledge base that will speed up their response. Therefore, the information that incident handlers rely upon must be accurate, up-to-date and easy to access.

This chapter will focus on the different aspects to consider when creating the documentation of your incident handling procedures: the guiding principles, planning, platforms and formats, collaboration strategies and style guidelines.

In the preparation phase of the incident handling process we try to have a set of articles, or playbooks, that allow us to respond to a set of incidents that we know, that we understand, or that happened in our helpline or in other organisations or CERTs. So we try to always have them ready for us, train our handlers to follow them, and when an incident that meets the criteria of that article happens, this is where the handler should go. If there is documentation for that kind of incident, then the handler should follow it.

Hassen Selmi, Incident Response Lead, Access Now Digital Security Helpline (Interview, November 2021).

The Basic Principles of Technical Documentation

The creation and maintenance of a DSHCS's technical knowledge base is an ongoing collaborative effort both within individual CERTs and helplines and in the community of digital security organisations for civil society at large. This collaborative effort has led to the adoption of some of the best practices established in the tech industry.

Whether it is an end-user guide for a phone app or a piece for the knowledge base included in a digital security helpline's ticketing system, every kind of technical documentation should be:

- Participatory: it should include everyone who will be using it, so there should be clear ways to contribute to it and all changes should be tracked.
- Current and updated: incorrect documentation can be more misleading than missing documentation.
- Unique: there should be only one place where the documentation is maintained, to avoid inconsistencies between versions.
- Discoverable: documentation needs to be found where it is needed.
- Comprehensible for its end users: technical slang should be avoided.
- Protected from unauthorised attempts at changing its content.
- Easy to reproduce for other projects.
- Easy to deploy to different formats: like websites, mobile apps or PDF files, among others.

Planning the Creation of New Documentation

A DSHCS can document technical solutions both for their incident handlers and for their beneficiaries, but sometimes writing can also be required for collaborations with partners, advocacy campaigns, media communications and so on.

Especially in the case when a piece of documentation is addressed to basic users, it is always worth asking whether the specific solution you want to document hasn't already been presented by other reputable digital security websites. If so, instead of writing from scratch, you could, for example, link a good resource to your knowledge base.

Before you start writing, it is a good practice to explore existing documentation, both to make sure that you aren't duplicating efforts and that you have a clear idea of the technical solutions required to solve a particular incident.

Once you have a good idea of what you want to write, try to develop your new piece of documentation so it can be used in other cases and is not specific to a case you've just seen. To do so, you can answer the following questions:

Who are you addressing?

Will you send this piece of documentation to individual beneficiaries by email or will you publish an advisory on your website for everybody to read? You could also be writing for incident handlers working in other organisations, for someone running an advocacy campaign or even for a talk at a specialised conference.

What do you want to accomplish?

Would you like your incident handlers to find quick technical solutions for the cases their beneficiaries are facing? Or are you writing a template for messages you often send to your beneficiaries? Are you preparing a security advisory to warn all your constituency about a new kind of digital attack? Or would you like to prepare a public report that can be sent to the media?

What kind of content best meets your audience's needs?

Consider the background of your readers. Are they IT professionals or basic users? Do they need accurate technical details or simple step-by-step instructions with screenshots? Will you need to add pictures to your guide or would it be even better to create a video or an infographic?

How will your content be found by its audience?

Will you include this content in your ticketing system? Will it be published on your website? Are you creating a manual that will be turned into a printable PDF or an app for mobile devices? Will your content be available both online and offline?

Will the content be translated or localised?

Based on your intended audience, you may want to translate your content to the languages and cultural references that are most used by the people you would like to reach.

By answering these questions, you can define the content, style and format of your piece of documentation. For example:

* If you need to warn your constituency about a new threat, you should write quickly and polish your message later.
* If the budget and timeline are tight, you might choose to share a simple

text with the relevant people as quickly as possible and think of a nicer format when resources are available.

- If the audience is large and the topic complex, a short video with subtitles might be helpful.
- If you are writing technical instructions for incident handlers, you should include technical details and make the documentation available in the same platform where your incident handlers document their cases (e.g. a ticketing system).
- If you are writing documentation that can be used by other civil society organisations, it is a good idea to use simple language that can be easily translated and publish your documentation with a licence and in a format that can be re-used by others.

Platforms and Formats for Technical Documentation

The most common tool used to develop documentation under the mentioned guiding principles, both in the IT industry and in the movement offering digital protection to civil society, is git, a technology for version control. In most cases, it is used with Markdown, a simple markup language (see below), and a static site generator to deploy the content to a searchable and user-friendly website.

Git for Version Control

Git is the most commonly used version control software for writing technical documentation collaboratively. Its main feature is to allow users to track the changes made to every file in a folder, so there is a record of every individual edit. It also allows reverting changes to a specific version, if needed.

Git makes collaboration easier by allowing to merge changes made by multiple people into one source. Another helpful feature of this software is the possibility to protect the collaborators' identities thanks to the option of creating private repositories that are only accessible to a selected group of users. Additionally, it allows to report issues, manage contributors, assign different roles, document the process, access analytics, etc.

Documentation managed in git repositories is usually hosted on third-party platforms like **Github** (**https://github.com**) or **Gitlab** (**https://gitlab.com**), or in self- hosted Gitlab instances. Some examples of git-based documentation developed collaboratively by civil society are:

- **Access Now Digital Security Helpline Community Documentation** (**https://communitydocs.accessnow.org/**) - deployed from this Gitlab.com repository: **https://gitlab.com/AccessNowHelpline/community-documentation**
- The Digital First Aid Kit: **https://digitalfirstaid.org** - deployed from this Gitlab.com repository: **https://gitlab.com/rarenet/dfak**
- SAFETAG - Security Auditing Framework and Evaluation Template for Advocacy Groups: **https://safetag.org/** - deployed from this Github.com repository: **https://github.com/SAFETAG/SAFETAG**

Although git is not complex for a regular contributor, some experience is required to get familiar with its logic and commands. There are many resources online to learn how to use git. Look until you find the one that best suits your learning needs. A good starting point can be *git - the simple guide*: **http://rogerdudler.github.io/git-guide/index.html.**

Markdown for Writing

In all the examples above, documents are written in **Markdown (https://**

daringfireball.net/projects/markdown), a lightweight markup language created by Aaron Swartz and John Gruber in 2004 to enable people "to write using an easy-to-read and easy-to-write plain text format, and optionally convert it to structurally valid XHTML (or HTML)".

Markdown documents can be converted into many different formats, allowing for the creation of websites, mobile apps, e-books and PDFs starting from the same source.

It is worth noting that, although most projects led by the civil society community use Markdown, other markup languages are used for technical documentation, in particular AsciiDoc (**https://asciidoc-py.github.io/index.html**) and reStructuredText (reST - **https://www.sphinx-doc.org/en/master/usage/restructuredtext/**).

If you are new to Markdown, you can have a syntax cheat sheet at hand for reference.

Learn more

Markdown guide **https://www.markdownguide.org/basic-syntax**

Github docs **https://docs.github.com/en/get-started/writing-on-github/getting-started-with-writing-and-formatting-on-github/basic-writing-and-formatting-syntax.**

Static Site Generators to CreateWebsites

To convert Markdown into searchable websites, static site generators like Jekyll (**https://jekyllrb.com/**), Gatsby (**https://www.gatsbyjs.com/**) or Metalsmith (**https://www.metalsmith.io/**) are commonly used.

Static site generators are an alternative to content management systems like WordPress or Drupal, where content is managed and stored in a database on the webserver. So instead of retrieving content from a database each time there is a request for web content, the static site generator deploys the entire website after each update and creates a tree of HTML files ready to visit.

A nice plus to this git-based infrastructure is that it is relatively simple to maintain. Static sites are robust against the attacks and trolling that are common in platforms like wikis - especially if they are open to editing by any user - or other web applications or dynamic websites, which require a lot of work to keep secure and make sure that content is not edited maliciously or by mistake.

Collaborative Documentation

By using a documentation infrastructure based on git, it also becomes possible for any other helpline or individual who has access to that git repository to use the same knowledge base to create their own website, mobile app, e-book, etc., and also to receive and submit updates to it.

This is made possible by the same architecture of git-hosting hubs like Gitlab or Github, which allows for making a copy of a project (**https://docs.gitlab.com/ee/user/project/repository/forking_workflow.html#creating-a-fork**) and submitting merge (or pull) requests to it after it has been changed in the copy, or "fork".

Given the limited amount of resources available in the civil society sphere to create technical documentation that is constantly updated, it has become an established practice to collaborate on shared technical documentation resources.

This requires avoiding formats that are not easy to download and duplicate and are not subject to version control, like wikis, websites, documents hosted on Google Drive,

or PDFs, and licensing content in a way that allows for collaboration and the creation of derivative works.

The collaboration approach also makes it possible to avoid duplicating efforts, as existing resources can be re-used instead of being written from scratch more than once.

Style Guidelines

Documentation of technical procedures for DSHCSs should be written in a language that is simple to read and inclusive, considering that often incident handlers are not English native speakers and that nobody is an expert on everything, especially in the civil society sphere.

In general, it's good to apply some basic rules that are recommended to all technical writers:

- Write short sentences that sound natural and friendly.
- Use common words as much as possible, don't use jargon or acronyms unless you really have to (and in that case, explain them at least once).
- Remember to be inclusive of all genders by using gender-neutral words and pronouns.
- Use active voice (actor + verb + target) as much as possible.
- Lists are a good resource for visualising information quickly.
- Link useful external resources in case the beneficiary needs more information on an issue.

There are many resources out there on how to write good technical documentation. What follows is just a short list:

Learn more

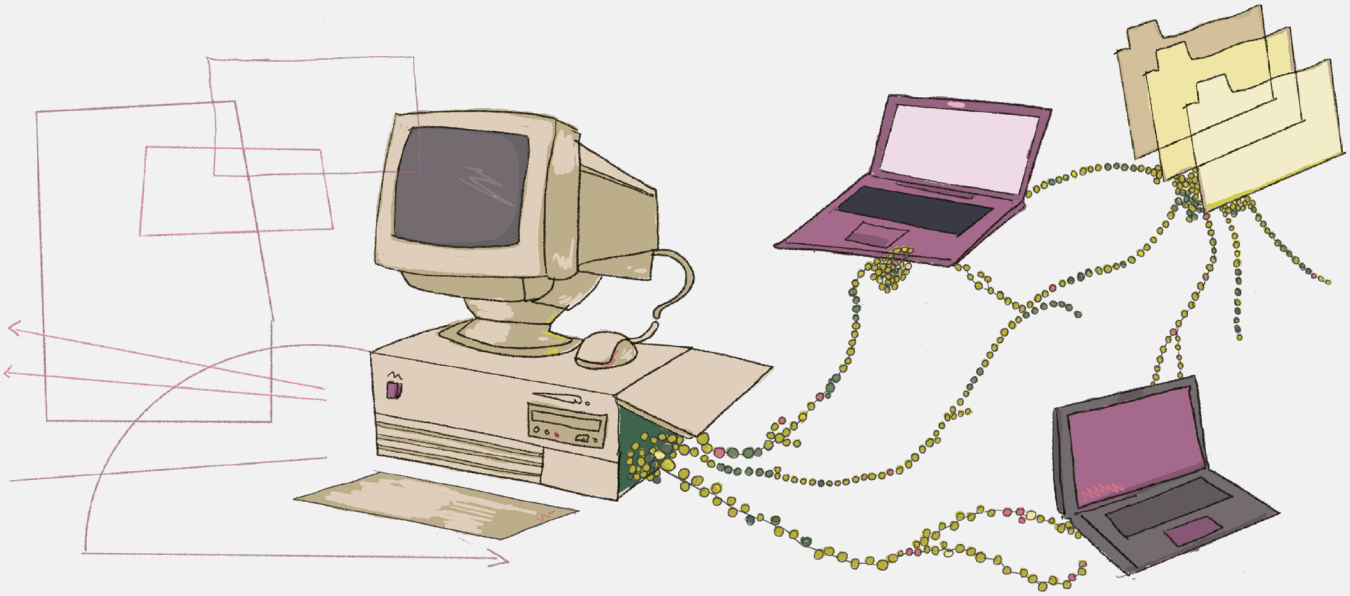
A list of technical writing resources in Google's Technical Writing Courses for Engineers: **https://developers.google.com/tech-writing/resources**

Microsoft Style Guide: **https://docs.microsoft.com/en-us/style-guide/welcome**

Tips on Bias-Free Communication: **https://docs.microsoft.com/en-us/style-guide/bias-free-communication**

Writing Step-by-Step Instructions: **https://docs.microsoft.com/en-us/style-guide/procedures-instructions/writing-step-by-step-instructions**

4



Beyond Your Team: Networking and Quality Assurance

Digital attacks are constantly evolving, broadening their scope of action and aggravating their impacts, as do the political contexts in which human rights defenders and activists operate. Keeping up with changes, understanding them and strategising responses can be time and resource consuming.

Creating and maintaining a community of practice is essential for a help desk as it enables collaboration. It also allows for more agile referral mechanisms, being aware of the realities of all regions, exchanging resources, learning about new approaches and producing collaborative research and investigations. Each help desk or CERT can specialise in a particular type of attack or constituency and the rest of the community members can benefit from that knowledge.

It is also important to keep constantly up-to-date, double-check that the procedures followed by incident handlers are appropriate, and receive continuous feedback from peers and beneficiaries to improve the help desk's workflow.

This chapter will focus on referrals, a common collaboration strategy among help desks and CERTs that allows scaling the response capacity towards civil society, and on quality assurance, with recommendations for different approaches and mechanisms that can be used to monitor, sustain and improve the quality of the services provided.

4.1 Create and Nourish Your Network of Partners

In order to have more referral options, it is important to build your web of trust, giving visibility to your work and knowing more about your peers' work. This can be achieved through participation in local and/or international events for instance. Whether online or at in-person events, you can present your work in booths, lightning talks, tech demos, community labs, workshops, etc. Check the conferences listed in **Chapter 2** (section on Training and Professional Development, p. 43) to know which ones to attend.

Being part of mailing lists such as the encrypted mailing list of **CiviCERT** (**https://www.civicert.org/about/**) is a huge asset, for example, when it comes to referrals. This community of digital security responders for civil society usually exchanges knowledge about referrals and rapid response expertise. Find more details about joining the network on their website: **https://www.civicert.org/apply-to-be-a-member/**.

It goes without saying that being part of a network or community is a proactive commitment. Communities need to be taken care of and nourished. In other words, they require maintenance of their infrastructure and documentation, facilitation of meetings, resources, outreach, exchange and, above all, time. Consider this when planning your team's hours and activities.

The detection of needs in the requests for support we received led us to create bridges with online platforms in the search to put a stop to the violence. We approached the platforms directly, and they opened their doors to us partly because there was information that interested them or because they wanted to connect with organisations that could mediate.
We had to be strategic and set limits on what information we shared because they used it to their advantage. If what they offered us was not intended to improve the care conditions for the women, we weren't interested. Even though they are big companies, we expect reciprocity in collaborations.

Luchadoras (Haché, 2021).

4.2 Referrals

Sometimes a DSHCS gets a request that they cannot handle, whether it falls outside their mandate or requires a set of skills the help desk lacks. The DSHCS may refer the case to another actor that can provide the support needed in such situations.

Once the requester is vetted, and depending on their request, you may direct them to 4 sorts of contacts:

- Another NGO or non-profit entity - This can be a referral to a non-profit organisation that you trust, know about, or have worked with in the past.
- Private companies - This can also be a referral to a private company with an ethical privacy policy and an ethical business model - a company that is trusted or familiar with non-profit challenges and that tends to use transparent and auditable open source technologies.
- Governmental entities - You might need to redirect to governmental institutions such as a national CERT.
- Freelance experts -You could also refer a beneficiary to an individual from the community of digital security experts who are familiar with human rights defenders' specific needs.

Below is a list of potential support you can find within or close to the digital security community once the need of the requester is identified. Vetting the requester is good practice when making a referral to a partner organisation's website but it is not mandatory in this case.

CERT teams (governmental institutions)

* FIRST Teams: https://www.first.org/members/teams

DDOS Attacks Prevention

* Deflect: https://deflect.ca/
* CloudFlare Galileo: https://www.cloudflare.com/galileo
* Google Project Shield: https://projectshield.withgoogle.com

Domains and Hosting

* Advice for hosting can be found in Access Now Helpline Community Documentation: https://accessnowhelpline.gitlab.io/community-documentation/88-Advice_Hosting.html

Emergency support

* Digital First Aid Kit, an intake mechanism to reach out to members of the CiviCERT community: https://digitalfirstaid.org/en/support
* Committee to Protect Journalists, for journalists: https://cpj.org/emergency-response/how-to-get-help

Funding and Free Licenses

* DDP Incident Emergency Fund: https://www.digitaldefenders.org/funding/incident-emergency-fund
* OTF Funds: https://www.opentech.fund/funds
* TechSoup: https://www.techsoup.org
* Google Nonprofits: https://www.google.com/nonprofits

Human Rights Violation Documentation

* Huridocs : https://huridocs.org/contact
* Witness : https://www.witness.org

Legal Support

* Media Defence: https://www.mediadefence.org

Physical Security and Relocation

* Protect Defenders: https://protectdefenders.eu/protecting-defenders
* Umbrella: https://secfirst.org/umbrella

Security Assessments and Penetration Testing

* OTF's Red Lab: https://www.opentech.fund/labs/red-team-lab

Training

* Training resources and references can be found in Access Now Helpline Community Documentation: https://accessnowhelpline.gitlab.io/community-documentation/301-Training_Resources.html

Referral Process

Vetting

Vetting the requester and their organisation is mandatory when referring someone directly to another team. During this process, you will need to ensure that you have verified the veracity of the request and the authenticity of the beneficiary's work and request. Vetting an organisation or individual is an opportunity to expand your and the community's web of trust.

Triage

Before referring to the appropriate organisation or individual, it is important to assess the requester's needs by starting to analyse their threat model and the incident they are experiencing. You may want to use a threat modelling or risk assessment approach as the entry point. This initial triage will help you figure out whom to refer the beneficiary to. Read more on how to do an initial risk assessment in Access Now Helpline's community documentation: https://accessnowhelpline.gitlab.io/community-documentation/200-Lightweight_Security_Assessment.html.

Identifying the Right Referral

The criteria of choice for a referral will be based on:

- The requester's needs
- The language used by the beneficiary
- The geopolitical context
- The technical expertise needed
- The cost of the referral

Get Consent For the Referral

It is recommended that you inform your beneficiary from the beginning about your intention to refer them to someone else. To comply with the confidentiality agreement between you and the requester, you should formally ask for their approval to share details with others (security assessment details, the beneficiary's identity and contact details, etc.).

Sharing with the requester key factors regarding the expertise of the entity you would like to refer them to and the main reasons you are opting for that specific entity, as well as the main reasons why you cannot fulfil the request, can help the beneficiary make their decision. The ability of the referral to provide pro-bono services or not is key and should also be mentioned in your communication with the beneficiary.

Get Consent From the Third Party You're Referring the Beneficiary To

Once the appropriate entity for your referral has been identified, and once the requester has approved the referral, you may share details with the third party you are referring them to regarding:

- The assessment of the requester's needs
- The requester's threat model

The goal is to make sure the third party you are referring the requester to has enough information to take the lead in handling the request. If the third party cannot provide a pro-bono service, the following details will need to be determined:

- What service will be offered
- The cost of the service

For a referral to be successful, these details will need to be discussed beforehand so that the beneficiary's and the referral's expectations match.

Establish the Connection

When putting the requester and referral in touch, try to identify a secure communication channel they are both familiar with. If they use PGP, consider sharing their PGP keys when introducing them to each other.

Follow-Up

After some time - depending on your workload, this may be a couple of weeks or some months - it is a good practice to check both with the beneficiary and the third party you referred them to in order to make sure their case was solved and their needs are fulfilled.

Referring an Open Case

It may happen that you have already begun helping a user at risk but for a variety of reasons you are no longer able to provide assistance to your beneficiary.

In such situations it is best to refer the beneficiary to a trusted partner. The referral process will follow the steps detailed in this section but should include an extra step to hand over the incident and an extra communication effort to manage expectations.

When updating your partner about your intention to forward them the request:

- Note that in this case, expectation management is key.
- Preferably have a list of referrals ready for these cases.
- Clarify financial details.

When agreeing with the requester to refer them to a partner:

- Explain why you need to refer them to someone else.
- Give them details about your partner's expertise.

During handover:

- Hand over to your partner all the information you have collected and your technical assessment.

4.3 Threat Information Sharing

It is a good practice to regularly share anonymised information on the cases you have handled with your community.

This exchange will allow other members to understand and identify digital attack patterns and trends that may also affect their beneficiaries.

At CiviCERT information on each member's work is shared bi-yearly based on the following questions:

Threat information

- What kind of rapid response cases have you dealt with in the past period of time?
- What was the nature of the attacks?
- Who was targeted?
- What trends do you observe in your work?

Threat Intelligence

- What recent threats and/or trends are you most concerned about?
- Has anything changed about the attacks you have been monitoring/addressing?
- What should other rapid responders be paying attention to?

Keep in mind that the anonymisation of this information has to be done in such a way that it is not possible to trace back the case in any way.

4.4 Quality Assurance

This process describes the recommended quality standards to be upheld by a help desk. It also presents recommendations for different angles and mechanisms that can be used to monitor, sustain and improve the quality of the services provided.

Quality Standards

In order to measure and evaluate the quality of your work it is important to define the expectations and standards that your DSHCS will use. The following guidelines should be considered when assessing the quality of the service:

- Create a space where beneficiaries and intermediaries feel welcome, understood, safe and secure.
- A help desk service should be clear, reliable and practical. Provide excellent customer service to your beneficiaries and deliver it in a manner that shows understanding and empathy to the needs of the beneficiaries and their situation.
- Treat beneficiaries with dignity, respect and confidentiality to ensure that they feel safe and secure and that their issue is being addressed.
- Listen first. Be patient and always listen to what beneficiaries have to say before jumping to conclusions and providing technical advice.
- Use clear, inclusive and gender-neutral language when writing or speaking.
- Incident handlers should adopt an approach informed by adult learning strategies. Whenever possible the aim of interactions should be to educate and empower the beneficiaries through knowledge and advice.
- Interactions with beneficiaries should be clear and concise. They may come from diverse backgrounds and have varying levels of technical proficiency.
- Define what will be your Service Level Agreement (SLA), which includes a maximum response time for incoming requests. For example, "respond to every request within the first two hours after it is received during work hours on a week-day, and within 24 hours during the weekend. See **https://en.wikipedia.org/wiki/Service-level_agreement**.
- Provide timely responses while a case is open. If a beneficiary becomes unresponsive, check in regularly to ensure their needs are met.
- Use the existing documentation, escalation processes and other mechanisms to provide excellent, reasonable and well-thought technical solutions.

Quality Assurance Mechanisms

Define Roles and Responsibilities

To be able to ensure the quality of the service, there are a few roles that need to be defined by the DSHCS.

Case owner: The person leading the case and working to help the beneficiary with their request.
Reviewer: The person in charge of reviewing the quality of the work. This may be the same person every time, or they may rotate among team members, depending on the size and structure of the DSHCS. For large organisations, there may be more than one reviewer.

Define a Time Frame

Case reviews need to be performed regularly to be effective. Define how often these reviews will be performed. The time range may vary from weekly to monthly, quarterly or even yearly reviews. The periodicity will depend on the size of the DSHCS, its staff capacity, the number of requests handled, the type of requests, etc.

Individual Case Reviews

Process

The reviewer will conduct a review of the cases closed by the case owners for the specified time period according to the DSHCS' needs.

Reviewers should have flexibility on when the review happens, but at the end of every period all closed cases should have been reviewed.

To facilitate the reviewers' work and get more valuable and useful reviews case owners should document each case thoroughly. Consider adding specific metadata to the case documentation to keep track of comments and feedback for each case. Also take note of any feedback or improvements that can be made to the review process itself.

The DSHCS should take review results into account to improve its policies, incident handling process, care protocols and team skills.

Criteria

The review will consider the following aspects:

Metadata

- Is all the case metadata complete?
- Is the content of the metadata detailed and accurate?

Timeliness

- Was the first response sent within the SLA?
- Were follow-ups made on a regular basis?
- Did the beneficiary receive responses in a timely manner?

Language

- Were communications with the beneficiary clear?
- Is the structure, spelling and grammar of communications adequate?
- Was the language used non-violent and gender-neutral? Was an intersectional approach adopted?

Proficiency

- Did the beneficiary undergo a risk assessment prior to recommending a solution?
- Was the solution used best suited to the beneficiary's context?

Documentation

- Was the case properly documented?
- Was any additional data (screenshots, analysis, files) properly recorded in the case?

Customer Service

- Was there an effort to validate the beneficiary's account of their story?
- Did the beneficiary feel empowered when the case was resolved?

Technical Recommendations

- Was the right technological solution applied in this case?
- Was the technical information communicated in a way that matched the beneficiary's capabilities and needs?

Feedback

A good way to constantly provide a good service to the beneficiaries is to implement some mechanism to gather feedback from them once the case has been resolved. This feedback can be collected in different ways, depending on your organisation's needs and capacities. Some examples are:

- Online forms
- Follow-up messages
- Debrief calls

It is important to keep in mind that the information gathered during this stage may be sensitive, so there is a need to ensure that it is securely transmitted and stored.

Feedback Review Process

If feedback is collected the reviewer should consider it and find possible areas of improvement for the processes.

The reviewer should then find a suitable way to report back to the case owner about this feedback (either positive or negative), and determine whether further actions are needed for the case in question.

References

Access Now Digital Security Helpline (2018). *Documentation for FIRST Site Visit*. Confidential.

Carnegie Mellon University (2004). *Creating and Managing Computer Security Incident Response Teams (CSIRTs)*. Carnegie Mellon University 1996-2004. **https://www.first.org/resources/papers/conference2004/t1_01.pdf.**

Cichonski, Paul, Millar, Tom, Grance, Tim, & Scarfone, Karen (2021). *Computer Security Incident Handling Guide*. NIST. **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.**

Dufkova, Andrea (2020). *FIRST Site Visit Requirements and Assessment.* FIRST. **https://www.first.org/membership/site- visit-v3.1.pdf**.

Eguren, Enrique, Cara, Marie (eds.) (2009). *New Protection Manual for Human Rights Defenders.* Protection International. **https://www.protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf**.

ENISA (2006). *A Step-by-Step Approach on How to Set Up a CSIRT.* **https://www.enisa.europa.eu/publications/csirt- setting-up-guide/at_download/fullReport**.

ENISA (2020). *How to set up CSIRT and SOC - Good Practice Guide.* **https://www.enisa.europa.eu/publications/how-to- set-up-csirt-and-soc.**

FIRST (2006). *CERT-in-a-Box*. GOVCERT.NL/NCSC. **https://www.first.org/resources/guides/cert-in-a-box.zip**.

FIRST (2019). *FIRST CSIRT Framework - Computer Security Incident Response Team (CSIRT) Services Framework*. **https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf.**

Haché, Alexandra (2021). *Models of Feminist Helplines for people facing Gender-Based Violence in Digital Spaces*. Digital Defenders Partnership. **https://www.digitaldefenders.org/wp-content/uploads/2022/01/VMD_EN.pdf**.

Higson Smith, Craig, Ó Cluanaigh, Daniel, Ravi, Ali G., Steudtner, Peter (2016). *Holistic Security - A Strategy Manual for Human Rights Defenders.* TacticalTechnology Collective. **https://holistic-security.tacticaltech.org/**.

INHOPE (2020). *Establishing a hotline guide,* INHOPE, **https://inhope.org/EN/hotline-guide**.

International Federation of Red Cross (2020) *Hotline in a Box.* IFRC. **https://www.communityengagementhub.org/wp-content/uploads/sites/2/2020/03/200325_Full-toolkit.pdf.**

International Organization for Migration (2007). *The IOM Handbook on Direct Assistance for Victims of Trafficking*. IOM. **https://publications.iom.int/system/files/pdf/iom_handbook_assistance.pdf.**

Kral, Patrick (2021). *Incident Handler's Handbook.* SANS Institute. **https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901.**

Maxigas (2014). Hacklabs and Hackerspaces: Shared MachineWorkshops. *Technological Sovereignty Vol. 1*. Passerelles 11. **https://www.coredem.info/rubrique48.html**.

Stratten, Kate, & Ainslie, Robert (2003). *Field Guide: Setting Up a Hotline. Field Guide.* Johns Hopkins Bloomberg School of Public Health - Center for Communication Programs. **https://pdf.usaid.gov/pdf_docs/PNACU541.pdf**.

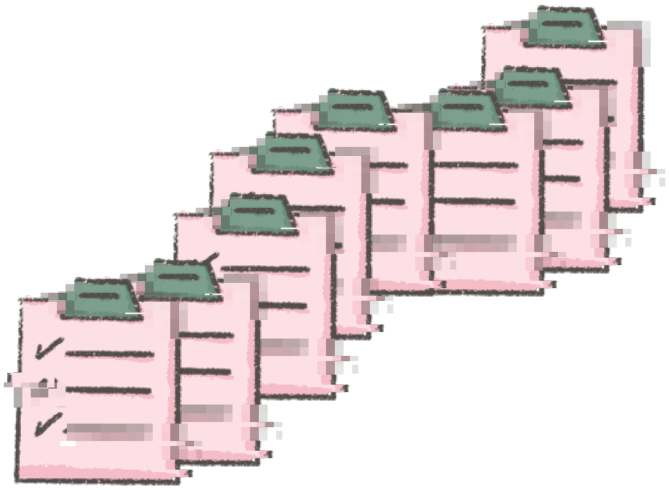
Tsunga, Arnold (ed.) (2007). *Protection Handbook for Human Rights Defenders*. Front Line Defenders. **https://www.frontlinedefenders.org/fr/file/1671/download?token=XHaqzSCK.**

United Nations Population Fund (2020). Guidelines for the provision of remote psychosocial support services for GBV survivors. UNFPA. **https://lac.unfpa.org/sites/default/files/pub-pdf/unfpa_guiavbg_web.pdf**.

Van der Heide, Martijn (2017). *Establishing a CSIRT*. ThaiCERT, ETDA. **https://www.thaicert.or.th/downloads/files/Establishing_a_CSIRT_en.pdf**.

West-Brown, Moira J., Stikvoort, Don, Kossakowski, Klaus-Peter, Killcrece, Georgia, Ruefle, Robin, & Zajicek, Mark (2003). *Handbook for Computer Security Incident Response Teams (CSIRTs).* Carnegie Mellon University. **https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf**.

Zimmerman, Carson (2014). *Ten Strategies of a World-Class Cybersecurity Operations Center*. MITRE. **https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf**.



Templates

Framework template

[Org Name]

1. Our Constituency

- Who are the beneficiaries of your DSHCS? Detail activity, field, gender, age, etc. The more accurately your constituency is defined the better you will be able to identify their needs and increase the quality of the service provided.
- What is the geographical scope of your constituency?
- Are there other DSHCSs providing services to the same constituency in your region? In such case what unattended needs will your DSHCS cover?

2. Our Constituency's Needs

If you decide, e.g., to support indigenous communities from a certain region, you could make a SWOT analysis to characterise them. For example:

	Helpful	**Harmful**
Internal	***Strengths*** They are very well organised and have access to a wide range of resources.	***Weaknesses*** Vertical structure centralises decision making.
External	***Opportunities*** Many International Cooperation Agencies are allocating funds to indigenous communities.	***Threats*** Increasing criminalisation of indigenous communities.

Now try using the same table for your beneficiaries:

	Helpful	**Harmful**
Internal	***Strengths*** Describe your constituency's strengths	***Weaknesses*** Describe your constituency's weaknesses
External	***Opportunities*** Describe your constituency's opportunities	***Threats*** Describe the threats affecting your constituency

You can complement the SWOT framework with a PESTLE analysis of the context in which your constituency operates.

Constituency	Political	Economical	Socio-Cultural	Technological	Legal	Environmental
Indigenous communities from X region	...	...	...	...	...	...

Threat Matrix

Likelihood / Impact	Low	Medium	High
Likely	...	...	...
Less Likely	...	...	...
Unlikely	...	...	...

Threat Inventory

Fill in a table for each threat identified in the threat matrix.

Title	
Description *Brief characterisation of the threat.*	

What	Target	Adversary	How	Where
The impacts the threat would cause	*What or who is the target*	*Who do you think is behind the threat?*	*The means by which the threat can come to fruition*	*What are the physical spaces the threat can manifest?*
...	...	...	...	...

3. Our Mission

What are your helpline's goals?Your mission statement should define your constituency, the situation you want to help overcome and how you plan to do it, as well as what services your helpline will provide.

Organisation Name - Mission

Describe your mission here:

.....
.....
.....
.....

4. Setting

- Will you be part of a larger organisation or constitute an independent project?
- Will you be volunteer-based or hire a team?
- How will your DSHCS will be funded?

5. Core Services

Service type	Service	Requirements
Reactive	*Equipment replacement.*	*Access to funding. Maybe we can refurbish old equipment for emergencies.*
Preventative	*In-Person Digital Security Training.*	*Need to find trainers in the area where the trainings will happen.*
...	...	...
...	...	...
...	...	...

6. Communication with your Constituency

Decide How Your Constituency Can Get in Touch

Channel	Advantages	Disadvantages	Accessibility for our constituency	Are we going to use it?
Form in website	*Easy to install. Can be encrypted.*	*Risk of spam.*	*Accessible.*	*Yes.*
Telephone	*Everybody can access a phone to call us.*	*SIM cards need to be registered with an ID.*	*Accessible.*	*No.*
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...

Declare Your Availability and Response Time

Operation hours:

- How will support requests outside of operational hours be attended to?
- How will the DSHCS prevent burnout of team members on call?

Decide How to Communicate withYour Constituency

- Will operators have an individual pseudonym or will they use a collective one?
- Does one operator always lead the communication with the person involved in a case? And if it is shared, is the conversation always conducted under the same pseudonym or does it change with each operator?
- Will the DSHCS adopt an informal tone or will operators keep their distance?

7. Policies

Policy	Description	Development and implementation	Responsible	Due date
1. Information Management Policy	*Procedures on how to manage and protect information.*	Yes	…	…
2. Incident Response Plan	*Roadmap for implementing the DSHCS' incident response capability.*	*Yes*	…	…
3. Vetting Policy	*Steps to verify new beneficiaries.*	Yes	…	…
4. Code of Practice	*Description of what is expected of the operators' behaviour.*	*Yes, but in a second stage*	…	…
5. Standard Operating Procedures	*Steps for responding to requests, making referrals, etc.*	*Yes*	…	…
6. Funding Policy	…	…	…	…
7. …	…	…	…	…

Code of Practice template

[Org Name]

Code of Practice

This code of practice applies to all *[Org Name]* spaces, either in online interactions or physical workspaces, associated events or social gatherings. Staff members and volunteers are responsible for knowing the values promoted by *[Org Name]*, which are detailed in this document and abiding by the rules detailed below.

The mission of *[Org Name]* is *[description of Org's mission]*. *[Org Name]* is committed to providing a safe and welcoming environment for realising this mission. In particular, we aim to banish any shame or stigma surrounding digital security mistakes or hacking, so we encourage all those involved to approach interactions with open, listening and supportive attitudes, and to engage constructively with others at all times.

More specifically, *[Org Name]* spaces are committed to promoting the following values:

> **Confidentiality:**We will handle all incoming information confidentially and will not disclose it to third parties without consent.We will handle incoming information responsibly and protect it against inadvertent disclosure to unauthorised parties. The security of the methods of storing and transmitting information inside or outside *[Org Name]* will be appropriate to its sensitivity.We invite all staff members and volunteers to read the *[Org Name]* policy regarding how information should be classified, stored, shared and destroyed.
> Any remote coordination or online initiatives will happen through secure channels that run on free and open source software and, especially if not end-to-end encrypted, are managed and hosted by trusted parties, ideally by *[Org Name]* itself. Commercial or proprietary tools will be avoided, especially if they have a history of violating users' privacy.
> **Collaboration:** We have a strong commitment to fostering solidarity, connection, cooperation and a sense of community in our spaces.
> **Inclusivity:**We believe in the importance of diversity in a way that fosters non-discrimination, free expression, participation and equality.
> **Do-No-Harm:**We are aware of how our actions, behaviours and ways of communicating can have a positive or negative effect on the people surrounding us and try to mitigate these as much as possible.We are aware of the elements affecting our own position of power and make space for acknowledging these structures within *[Org Name]* spaces. *[Org Name]* is dedicated to providing a harassment-free experience for everyone, regardless of gender, gender identity and expression, age, sexual orientation, disability, physical appearance, body size, race, ethnicity, religion (or lack thereof), technology choices, skill set or level of knowledge.We do not tolerate harassment in any form. Anyone who violates this code of conduct may be sanctioned or expelled from these spaces at the discretion of *[Org Name]*.

Harassment

Harassment may occur online or in person. Examples of unacceptable behaviour include:

1. Offensive comments which reinforce social structures of domination and/or are related to gender, gender identity and expression, sexual orientation, disability, mental illness, neuro(a)typicality, physical appearance, body size, age, race or religion.

2. Offensive comments and flamewars about other people's choices of recommended practices, skills, procedures and tools.
3. Unwelcome comments regarding a person's lifestyle choices and practices, including those related to food, health, parenting, drugs and employment.
4. Deliberate misgendering or use of 'dead' or rejected names.
5. Gratuitous or off-topic sexual images or behavior in spaces where they're not appropriate.
6. Physical contact and simulated physical contact (e.g., textual descriptions like "hug" or "backrub") after a request to stop. Threats of violence.
7. Incitement to violence towards any individual, including encouraging a person to commit suicide or to engage in self-harm.
8. Deliberate intimidation.
9. Stalking or following.
10. Harassing photography or recording, including logging online activity for harassment purposes.
11. Sustained disruption of discussions, talks or other events.
12. Unwelcome sexual attention or physical contact.

Patterns of inappropriate ***social*** contact, such as requesting/assuming inappropriate levels of intimacy with others.

13. Continued one-on-one communication after requests to cease.
14. Deliberate "outing" of any aspect of a person's identity without their consent, except as necessary to protect vulnerable people from intentional abuse.
15. Publication of non-harassing private communication.
16. Publishing another person's private information, such as physical or electronic addresses, without explicit permission.
17. Advocating for, or encouraging, any of the above behaviour.
18. Drugging food or drink.
19. Violating the privacy policy of an event in order to attract negative attention to an attendee.
20. Enlisting the help of others, whether in person or online, in order to target someone. We prioritise marginalised people's safety over privileged people's comfort

Our team will not act on complaints regarding:

- 'Reverse' -isms, including 'reverse racism,' 'reverse sexism,' and 'cisphobia'.
- Reasonable communication of boundaries, such as "leave me alone," "go away," or "I'm not discussing this with you."
- Communicating in a 'tone' you don't find congenial.
- Criticising racist, sexist, cissexist, or otherwise oppressive behaviour or assumptions.

NOTE:
- Let someone leave a conversation that makes them uncomfortable, and do not follow people who asked to be left alone.
- If you discuss difficult topics that may be traumatic for participants, provide warnings so people may leave a conversation or plan coping strategies.

Reporting

If you are being harassed, notice that someone else is being harassed, or have any other concerns, please notify us by sending an email to *[dedicated email address]*. Currently, there are *[n.]* persons receiving these emails: *[Names]*. Reports are confidential. You will not be asked to take actions that make you feel unsafe.

This code of practice applies to *[Org Name]* spaces but if you are being harassed by a person involved in *[Org Name]* outside our spaces we still want to know about it.We will take all good-faith reports of harassment seriously. This includes harassment outside our spaces and harassment that took place at any point in time.

The response team will contact the accused person in order to inform them about the process and give them an opportunity to respond. The response team reserves the right to exclude people from *[Org Name]* based on their past behaviour, including behaviour outside *[Org Name]* spaces.We will respect confidentiality requests for the purpose of protecting victims of abuse. At our discretion we may publicly name a person about whom we've received harassment complaints, or privately warn third parties about them, if we believe that doing so will increase the safety of partners or people involved with *[Org Name]*.We will not name harassment victims without their affirmative consent.

Harassment and other code of practice violations reduce the value of our community for everyone.We want you to be happy in our community as people like you make it a better place. If the person who is harassing you is part of the response team or *[Org Name]* management, they will recuse themselves from handling your incident.We will respond as promptly as we can.

Consequences

Staff members or volunteers asked to stop any harassing behaviour are expected to comply immediately. If someone at *[Org Name]* engages in harassing behaviour, the response team may take any action they deem appropriate, up to and including dismissal and identification of a staff member or volunteer as a harasser to the general public.

Licensing

Incident Response Plan Template

[Org Name]

Incident Response Plan

This process describes the way in which *[Org Name]* receives and responds to computer security incidents. This process covers how incidents are assigned, analysed, managed, escalated, closed and reviewed for lessons learned.

Receiving and assigning incidents

Whenever an incident is received an incident handler is responsible for providing an initial response and ensuring the incident is followed through. This first response should be provided as soon as possible, and must always happen within *[time defined by the DSHCS's service level agreement]*.

The case owner is responsible for the analysis of and response to the incident. The criteria to define the case owner should include:

- Case priority
- Language of the case / languages spoken by the incident handlers
- Incident handlers' case loads
- Geographic location of the beneficiary / time zone
- Skill set required to resolve the incident

Shift leaders are responsible for balancing the workload within and across offices. If necessary an incident handler can request that a case be owned by a different person, in case the new case owner is better suited to deal with the ongoing incident. This should be done in agreement with the current and future owner. If necessary the beneficiary should also be informed of the change of ownership.

Assigning case Priorities

Case priority refers to a value assigned to each case. Priorities help case owners and, generally, the DSHCS team manager to allocate the right amount of resources for each case. They also define the order in which cases should be resolved. Priority reflects the organisational response required for each request.

Among the variables involved in prioritisation, impact and urgency are the most relevant.

1. Impact for the Beneficiary

In instances where the beneficiary is in danger, physically or digitally, and the consequence of not acting is severe, the case should be addressed by the incident handler by considering the possible consequences and effects of the issue and the solution to be proposed. There are three categories for case impact: high, moderate and low impact.

To establish a case's impact, a guide table is presented below:

Category	Description
High (H)	- Someone has been or is at risk of being injured - The beneficiary is dealing with a reactive/dangerous situation - There is a high risk of sensitive information being compromised - Personal information of several beneficiaries is likely to be compromised - The damage to the help desk's reputation is likely to be high if the situation isn't handled properly - The beneficiary might be a high-profile person
Medium (M)	- The consequences caused by the incident can be defined as an intermediate value between low and high
Low (L)	- The case aims at preventing a future security incident for the organisation - The consequences of the help desk's advice do not translate into an imminent physical damage to the beneficiary

2. Impact for the DSHCS

Sometimes cases might impact the help desk and its reputation. These cases need to be handled with special care, involving the management team in their resolution.

3. Urgency

This is defined as the amount of delay that can be tolerated and how quickly a solution is needed. Cases can be classified as highly urgent, moderately urgent and not urgent. This will depend on various factors, including the timelines involved and the level of threat if action is not taken within a certain time frame.

To establish case priority incident handlers should also consider what the beneficiary mentions when opening the case.

Sometimes beneficiaries specify that the case is urgent for a particular reason.To establish case urgency, a guide table is presented below:

Category	Description
High (H)	- The consequences caused by the incident increase rapidly over time -A minor incident can be prevented from becoming a major incident by acting immediately - The case was opened in a reactive manner, by a beneficiary seeking for immediate assistance - Is it a DDoS? Is there an ongoing data breach?
Medium (M)	- The consequences caused by the incident increase slowly over time
Low (L)	- The consequences of not solving the case do not increase over time - The case aims at preventing a future security incident for the organisation

4. Priority

By combining the above-mentioned factors (urgency and impact) the incident handler can assess the corresponding case priority. This priority is listed in the table below:

		Impact		
		High	Medium	Low
Urgency	High	1	2	3
	Medium	2	3	4
	Low	3	4	5

NOTE:
If there is any doubt about the urgency or impact of a case, it is always best to err on the side of caution and not to take any risks.

As a rule, if a case has a higher priority, it also has a significant impact for the help desk and the beneficiary. Note that no matter what priority the case has, if the incident handler is unsure about the advice they should give they must request support from colleagues.

Incident Response Life Cycle

The following is our incident response workflow. This provides a general overview of how digital security incidents should be managed. It doesn't provide advice on how to tackle specific incidents. For specific advice on how to manage different types of incidents, please refer to our procedural documentation.

The incident response life cycle followed by the help desk is based on: Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, *Computer Security Incident Handling Guide*, NIST, 2021. (**https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf**).

When an organisation reaches out to our DSHCS asking for preventative support, they are often **preparing** and adjusting their practices to prevent digital security incidents from taking place. This is the ideal scenario, where we help our beneficiaries mitigate the risk of compromise of their security or data.

On some occasions the beneficiary's request is to investigate a potential incident or attempted incident. These types of reports do not include clear evidence that an incident has already happened and thus require an initial investigation to verify the reporting and confirm if an incident has already taken place or not. This phase is called **detection** and the handler may require more evidence for their investigation until it is clear for them whether this event indeed compromised the beneficiary's security, or if it was just an event without consequences. Our procedural documentation should help the handler understand what evidence or information is helpful to investigate different types of incidents.

These types of cases will normally be of medium or high urgency, especially while still determining if an incident took place or not.

However, often beneficiaries reach out to our help desk when an incident has already taken place. This means there has been one or multiple actions that intentionally harm or attempt to harm the beneficiary's system, network or data.

Examples can be: system unavailability, data leak, device seizure, account compromise, etc. Therefore, we normally prioritise the **containment** of that incident to stop harm from spreading to other parties.

Actions that we often take to **contain incidents** include: requesting an online platform to suspend a compromised account, isolating a compromised system from the network, suspending a defaced website, removing leaked data, etc.

Containment should be quick in most of the cases and it should be prioritised. In some cases, we will rely on the beneficiary's actions to remove their system from the network or isolate it while we provide the technical instructions via remote communications. Urgency will normally be high in cases where we are trying to contain an incident that is taking place.

When containment is achieved, it is often important for the case owner to dedicate some time to analyse the root cause of the issue. This normally leads to an investigation that usually takes place under the **detection and analysis** phase.

Depending on the category of the case, additional evidence could be requested from the beneficiary to perform **analysis**, such as the source of received recently malicious email, the link to download a malicious app, screenshots of antivirus alerts, etc. The goal here is to determine if there are any additional actions that should be taken to ensure that the recovery from the incident is substantial. Again, the handler should refer to our procedural documentation to know what other information can be helpful to perform their analysis.

Eradication consists in cleaning any compromised systems to ensure a substantial recovery. It could be as simple as installing and running an antivirus application or in some other cases it could require a fresh system install. However in all cases, it is essential to know and document what - if anything - the attacker left behind and clean it. This is useful in order to monitor the attacker's possible comeback and also to look for other similar attacks against other systems or beneficiaries. For systems that cannot be installed again or cannot be reset to factory settings, the attacker's artefacts that are identified in the analysis phase can be removed manually: think of startup or cron tasks to relaunch a backdoor. In cases such as DDoS attacks, **eradication** is not possible because in such incidents the attacker does not leave any artefacts and the source of the attack is so distributed that taking down every implicated host in the attack is neither possible nor reasonable. However in cases where the attacker's infrastructure is not distributed, taking down this malicious infrastructure should be considered part of the eradication phase. Reporting an account that is leaking information or suspending an email address that is sending phishing emails could also be considered **eradication**.

Eradication usually should not be urgent as the threat should be already contained at this stage. However if the system continues to be live or connected (according to the owner's preference) and the analysis has discovered artefacts that allow the attacker to return soon or immediately, the urgency of the case should be marked as high.

The distinction between the recovery and eradication phases is not always clear, as you end up recovering from the incident by just eradicating the attacker's artefact: think of removing the hacker's email address or phone number from the account and associate it to legitimate ones or using an antivirus to clean a non persistent worm. However, to ensure recovery it is important, in some cases, to monitor for any comeback from the attacker. This task should be considered especially important when we discover that the attack is highly targeted and the threat is persistent. In these cases, attackers won't hesitate to attack again using the same vulnerability/weakness or by looking for other ones. Depending on how feasible it is to do so, you can help a beneficiary monitor for any of the artefacts that have been already found and removed in the eradication phase.

Post-incident activity consists in preventative work that can be performed following the attack. It could be training, system hardening, penetration testing, a security audit and assessment of the beneficiary's organisation, among other things. How-

ever some of this preventative work could be done earlier in the incident's life to ensure a substantial recovery too. For example, a beneficiary whose account has been hacked could be assisted to create a new email address protected by a strong password and 2-factor authentication to be able to recover their account. In cases of system compromise, a vulnerability scan could be conducted on the system to close any vulnerability that allows further attacks before this system is back to production. In harassment cases open source intelligence research could help a victim recover from a previous harassment attack, to identify any available online information that could be used by the attacker again. Post-incident activity cases that are required to recover from the incident should never be marked as low urgency cases!

Important Considerations

The following notes should be considered when responding to requests:

- After a case is received, in addition to the automatic reply sent by the ticketing system, the operator on shift should personally answer the case requester, explaining they will be in charge of the case and making themselvesavailable for any issue that arrives.
- Vetting a new beneficiary could take some time. While this process is taking place the owner of the case should begin working on the solution, considering that while the beneficiary is not vetted extra care should be taken as to what information is shared and what actions are taken since we haven't yet confirmed the link of trust.
- When looking for solutions for cases, please always consider the following suggestions:
  - Look for related procedural documentation.
  - Escalate to other colleagues and/or consider reaching out to partner organisations for specific cases.
  - Consider reaching out to CiviCERT.
  - In case you reach a dead end, always escalate and discuss the case with your manager.

Reasons for Closure

When closing a case the incident handler should record the reason for closing it. The possible options are:

- **Successfully Solved:** Case goal was successfully completed.
- **Customer unresponsiveness:** The beneficiary was not responsive after several communications.
- **Future Improvement:** Case goal was not fully completed and further actions will be carried out in the future.
- **Unsuccessful solution:** Case goal was not met.
- **Customer Request:** Customer explicitly requested the closure of the case.
- **Internal Case Cancellation:** Case was cancelled after request from internal team member.

A case should only be closed due to a lack of response from the beneficiary if that unresponsiveness stops us from meeting the goal of responding to the incident. If the incident handler has met the requirements to complete the case, then the case should be labelled as successfully solved, regardless of whether we hear back from the beneficiary or not.

Information Management Policy Template

[Org Name]

Information Management Policy

1. Information Classification

[Org Name] supports the Information Sharing Traffic Light Protocol.

Data classification description

PUBLIC: This information is deemed to be non-sensitive (meaning that it excludes personal data and details on collaborations with third parties and internal procedures) and can be distributed to anyone in any context. The information is intended for public consumption. It may have already been reported on, and/or is available to be reported on.

CONFIDENTIAL: Information marked as confidential can be shared to other *[Org Name]* teams, as well as to trusted third parties on a need-to-know basis, i.e. only if a specific case can only be addressed by sharing information with them. By default the information is only shared among *[Org Name]* staff members. There should be no assumption about sharing the information to third parties, and this kind of information should only be shared on a need-to-know basis with third parties that have signed a non-disclosure agreement which includes minimum standards around data storage and retention that aligns with [Org Name]'s Retention Policy (see below).

RESTRICTED: *[group / entity / list of individuals]* – Any information classified as restricted must also include a group, entity, or list of individuals that the information is to be restricted to. When the information is restricted to groups or entities, any individual's membership in that group or entity means that that individual has access to the information. Restricted information can also be shared with third parties on a need-to-know basis. So for "RESTRICTED: *[Org Name]* tech team" these other parties may be the beneficiary, as well as another third party that needs to be involved to solve a case. Some information is so sensitive that it should only be shared with individuals on a must-need-to-know basis. In that case, this information will be labelled as "RESTRICTED: *[list of individuals]*". This information is never shared with groups, so group membership never grants access to this classification of information. When emailed, only the named recipients of the email are considered the "need-to-know" individuals, and the information must not be shared beyond those named recipients.

Color	Classification	Scope	Examples
RED	*RESTRICTED [list of individuals*]	Named individuals.	· legal requests. · trust issues.
AMBER	*RESTRICTED [entity]*	Membership of ***[entity]*** and need-to-know 3rd parties.	· requests by beneficiaries. · case history data (which may include personal data necessary for the delivery of services). · personal contacts (if necessary and justified by a request from members of entity and third-parties). · documentation on internal infrastructure. · documentation on internal procedures.
GREEN	*CONFIDENTIAL*	***[Org Name]*** members; need-to-know 3rd parties.	· civil society threat intelligence. · documentation on escalations and procedures.
WHITE	*PUBLIC*	All.	· general security recommendations. · blog posts. · website content. · social media posts.

2. Information Protection

- Public information can be widely distributed and takes the form of newsletters, website content, social media posts, information on public malware information sharing platforms, etc. ***[Org Name]***'s infrastructure hosting public information is hardened and protected against the compromise of the integrity of such information. All public data is backed up against loss of such information.

- Confidential information is stored in platforms that are only accessible by ***[Org Name]*** staff and can be shared with third parties on a need-to-know basis. Access to these platforms is password-protected and 2-factor authentication is required whenever possible. This kind of information is also stored in work devices with full-disk encryption. This kind of information is only transferred through end-to-end encrypted channels of communication.

- Restricted information

  Information restricted to single *[Org Name]* teams is only stored on password-protected platforms and in work devices with full-disk encryption. This kind of information is only transferred through end-to-end encrypted channels of communication.

  Information restricted to individuals is only stored on password-protected platforms and is only transferred through end-to-end encrypted channels of communication.

Individual staff members' GPG private keys are only stored in their devices laptops with full-disk encryption or in fully encrypted external storage media.

The security measures put in place for the protection of information are minimum standards and, as they are also evolving, may change in the future.

3. Information dissemination

Information that may not be shared:

- Incoming information restricted to specific individuals will not be shared beyond those named recipients.

Limitations to this policy:

- Information may be shared in compliance with national and international legal obligations, including in response to requests from law enforcement that compel *[Org Name]* to produce records. *[Org Name]* will vigorously challenge legal orders or other requests that infringe on human rights and will exercise whatever power we have to protect our beneficiaries, partners and staff.

4. Access to Information

Legal requests by law enforcement authorities, communications on trust issues and other critical information may be labelled as RESTRICTED to single individuals and disclosed only on a need-to-know basis, until it becomes possible to lower the confidentiality level of this information.

Changing the classification of data

Information classified as CONFIDENTIAL can become public only after removing all sensitive information or under explicit authorisation of the individuals and groups mentioned in the information. If information is classified as confidential to grant exclusive publication rights, it will automatically become public as soon as it has been published.

5. Cooperation with other teams

This policy defines the process followed by *[Org Name]* to engage in formal or informal cooperation with other CERTs and digital security response teams for civil society.

- *[Org Name]* can share information classified as "PUBLIC" in any forum where any CERT or digital security response team for civil society have access.
- If *[Org Name]* determines the best action on behalf of a beneficiary is to engage with a specific other CERT or digital security response team for civil society, those communications and associated data should be considered "CONFIDENTIAL", or "RESTRICTED: ***[list of entities]***" (see "Information Classification" above).
- In such cases, *[Org Name]* will secure the permission of the beneficiary in order to pursue resolution of their case through the services provided by another CERT or digital security response team for civil society.
    In some instances *[Org name]* will not secure the permission of the beneficiary as that permission can be assumed, for example in cases like the following:
    - » If the beneficiary has instructed the CERT or digital security response team for civil society to pursue the takedown of a phishing content host (note that before taking such cases towards takedown resolution, our processes relating to threat intelligence coordination, and pursuing the most beneficial actions for the largest number of interested parties in such circumstances, should be followed first);
    - » Account recovery or deactivation (assuming that vetting of the beneficiary has occurred) with the CERT of the platform involved;

    - A shutdown complaint, if that shutdown has affected the general public.
- Circumstances where we absolutely require a permission from the beneficiary include:
    - C&C server takedown;
    - Malware analysis, particularly where a device is to be examined;
    - Censorship resolution.

6. Record Retentions

All information shared within *[Org Name]* is stored in *[Org Name]*'s own servers, for which the following policy applies:

Retention Policy

All information in *[Org Name]*'s infrastructure, including threat information, requests from beneficiaries and partners and internal documentation, is stored for as long as necessary in *[Org Name]*'s servers, for the purpose of information sharing and delivery of services and for compliance with national and international legal obligations, including the prevention of criminal offences and the enforcement of civil law claims.

All information in *[Org Name]*'s infrastructure, except for public information which is non-sensitive and does not include any personal data, is stored on password-protected platforms and in work devices with full-disk encryption. This kind of information is only transferred through end-to-end encrypted channels of communication. These are the minimum standards in place and, as they are also evolving, may change in the future.

Data Breach Policy

In case of a personal data breach which is likely to result in a risk to the rights and freedoms of the data subjects, *[Org Name]* shall notify the data subjects without undue delay and also notify the supervisory competent authority, without undue delay and where feasible, no later than 72 hours after having become aware of the breach, in accordance with the EU's General Data Protection Regulation.

In addressing data security breaches, *[Org Name]* shall take measures to mitigate damage, investigate, conduct remedial action and comply with regulatory requirements for information security.

7. Data destruction process

Physical documents

Printing should be limited to a minimum. Printed documents should be stored only as long as needed and it is recommended not to cross borders with confidential or restricted printed papers.

Physical paper documents containing CONFIDENTIAL information should be destroyed in a ribbon or cross-cut shredder, while any other physical documents containing RESTRICTED information must be shredded with a cross-cut shredder.

Storage devices

Hard drives, USB thumb drives, and other portable storage devices containing CONFIDENTIAL or RESTRICTED information should be securely erased with a single pass of clearing process: random data (/dev/urandom) before they are thrown out. Write-once CDs should be broken into pieces or destroyed in the shredder before being thrown out.

Digital data

Digital files containing CONFIDENTIAL information can be simply deleted, while for RESTRICTED data a minimum of one clearing process must be done over the file.

8. Appropriate usage of work devices

All *[Org Name]* members make sure that the devices they access *[Org Name]* information with are protected with full-disk encryption and used according to sound judgement, with regular updates of the system and software and other measures to prevent infection or unauthorised access to the system and accounts.

9. *[Org Name]*'s Communications and PGP Policy

"RESTRICTED" information should only be shared with other *[Org Name]* staff members over strongly encrypted channels, such as PGP-encrypted email, Signal, or similar.

[Org Name] supports PGP-encrypted communications and communicates over an encrypted channel.

It is mandatory for all [Org Name] staff members to use PGP/GnuPG for encrypting every email communications with:

- other team members
- third parties, when exchanging confidential and restricted information

It is recommended that PGP key pairs used for communicating with *[Org Name]* team members and third parties have the following settings:

- Algorithm: RSA
- Key length: 4096
- Expiration Date: 5 years
- Private key protected by a strong password, consisting of at least 20 characters, including lower- and upper-case letters, numbers and symbols, or a passphrase created with the diceware method, with at least 6 words

Should a device containing a PGP private key be stolen, or should a PGP key pair be otherwise compromised, the key pair will be revoked as soon as possible and [Org Name] management will be notified.

Vetting Process Template

[Org Name]

Vetting Process

Purpose of vetting

The purpose of vetting beneficiaries is an exercise in reducing risk for *[Org Name]* and for users at risk.

Some of the risks mitigated by vetting include the risk to *[Org Name]* of reputational damage resulting from working with orga nisations that themselves do not uphold basic human rights, or are controversial for any other reason. There is the risk of being socially engineered by our adversaries into releasing information, or allowing our adversaries into getting a foothold onto our platforms, that would then allow them to perpetrate effective attacks on our operation. There is also the risk of adversaries consuming our resources in fake incidents, thus denying capability to the people and organisations that really require our assistance.

Vetting is an exercise of doing adequate due diligence with the beneficiaries we assist to ensure they are truly part of our constituency.

To make sure this vetting process is properly recorded all communications needed to complete the vetting process will be recorded in a chronological order in the case history.

[Org Name] Vetting Process

The process used to vet all new beneficiaries consists of the following steps:

1. Initial evaluation
2. Identify/contact potential vettors
3. Evaluation of responses
4. Sign off and recording

1. Initial evaluation

A certain amount of groundwork can be done initially via information sources such as Google, Wikipedia, the requester's own website, Whois, PGP keyservers, etc., to make a determination of the validity of the organisation and individual/s in question. None of these sources alone should be considered reliable, but putting them together makes it possible to get some sense of the legitimacy of the organisation/individual.

2. Identify/contact potential vettors

Identifying potential vettors is the next step.We need to find someone we already know and trust that is prepared to vouch for the potential new beneficiary.

A good place to start is to look at the organisation's website, particularly any pages identifying members of the organisation's board. Board members are often high-profile people in the NGO space and are frequently known to staff at *[Org Name]* or to partners, so this presents an excellent way to identify potential vettors.

3. Evaluation of responses

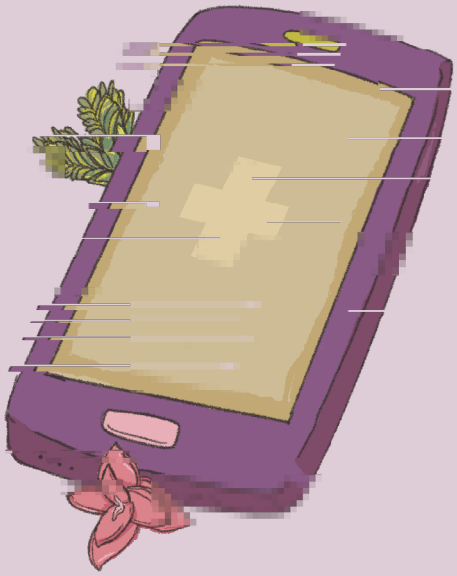
What we are trying to establish is that the beneficiary is who they claim they are, and that they act rationally and with safety and respect for others. It is important that the beneficiary has the capacity to respect *[Org Name]*'s reputation if we are to involve our organisation in providing them assistance. For us this is largely what we are trying to determine.

This is never going to be a hard and fast ruling on "adequacy", as the nature of trust relationships will always be somewhat subjective. However as a general heuristic rule we can consider that if someone we trust implicitly vouches for a new beneficiary we can consider them vetted. If we cannot find someone that we trust implicitly, then we would need two acquaintances whose reputations we trust, that both vouch for the new beneficiary before we would consider the vetting adequate.

4. Sign off and recording

Each vetting process needs to be signed off by the *[roles of team members in charge of signing off vetting processes in the organisation]*.

The fact that the beneficiary has been through the vetting process and either been declined or successfully vetted is recorded in the case history.



Digital
Defenders
Partnership

CiviCERT