USAID FROM THE AMERICAN PEOPLE | PROgress PROTECTING GLOBAL RIGHTS | Freedom House | Internews Local voices. Global change.

WHAT IS THE DIGITAL SECURITY FRAMEWORK (DSF)?

HUMAN RIGHTS SUPPORT MECHANISM PROGRAM

This Digital Security Framework was developed by Freedom House and Internews as part of the USAID-funded Human Rights Support Mechanism (HRSM).

Report period: January 2022 – May 2023

Published: June 2023

Freedom House and Internews would like to thank USAID for its commitment to the HRSM learning agenda. Freedom House and Internews wish to extend their particular gratitude to HRSM program teams and partnering human rights organizations across the globe who contributed their invaluable time and input for the development of this learning product. Thanks are also owed to the many digital security and program experts who reviewed this document to ensure it was technically sound. Due to security considerations, not every contributor is listed by name.

Authors

Megan Guidrey | Director of Monitoring and Evaluation, Internews

Deanna Kolberg-Shah | Evidence & Learning Team Technical Lead, Freedom House

Leah Squires | Monitoring, Evaluation, and Learning Specialist, Freedom House

Expert Reviewers

Ashley Fowler | Senior Manager of Internet Freedom & Resilience Programs, Internews

Łukasz Król | Journalist Digital Security Specialist, Internews

Rafael G. Nunez | Senior Program Associate, Freedom House

Cover Image:
A group of men track presidential election results on their phones at the Gikomba market in Nairobi, Kenya, in August 2022. (*Credit: Alamy*)

What is the Digital Security Framework (DSF)?

There is no universal means to assess digital security needs, implement digital security supports, or measure digital security interventions since any approach is highly contextual. This reference offers a logical framework for digital security support. It is intended for use by democracy, human rights, and governance implementing partners to assist in the design, implementation, and monitoring and evaluation of digital security activities with human rights organizations (HRO), including civil society organizations or media outlets that focus on human rights issues.

This framework describes three main types of digital security interventions, reflecting digital security assistance that is likely achievable based on typical award timelines in human rights programming:

Emergency Interventions	Refer to an incident response around an immediate, specific threat or an attack that an organization has already experienced. While rapid data recovery or other emergency interventions last only days, programs that last less than eight months likely can only respond to a series of emergency requests. During this time, HROs may also receive targeted education and corresponding mitigation and/or prevention tools that help them survive the particular threat or attack. In an operating context where there is an immediate threat, i.e., ongoing surveillance, implementing partners should include incident response capabilities in the program design.
Short-term Interventions	Include ongoing support from the same digital security experts to HROs for a period of nine to twelve months. Activities can include emergency support, capacity assessments, and training and mentorship. While emergency interventions prioritize building an HRO's awareness or knowledge around a specific incident, short-term interventions can address both immediate needs and broader digital security issues.
Long-term Interventions	Aim to improve holistic digital safety and security practices that better equip partners to respond to increasingly advanced digital threats. These year-plus programs incorporate activities typical of a short-term intervention, beginning with a focus on immediate needs and general digital security know-how. With a longer timeline, these interventions are distinguished by depth over breadth, progressing to implement more sophisticated assessments, as well as mitigating and preventive, context-specific solutions to address complex digital security threats.

The DSF identifies three core digital security outcomes that can be measured as a result of digital security program assistance:

1. **Awareness** refers to changing participants' beliefs that digital threats pose a legitimate risk to organizational and personal safety.

2. **Knowledge** refers to changing participants' understanding of different digital security threats and the appropriate actions and tools to mitigate those risks. Knowledge development distinguishes itself from awareness raising because it requires a deeper understanding of threats and tactics, i.e., identifying which threats are most likely in a given context, and then prioritizing mitigation and preventative measures that are commensurate with the threat environment.

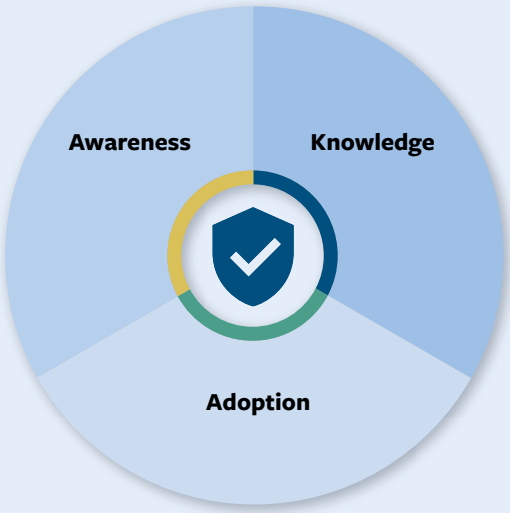
3. **Adoption** refers to changing participants' abilities and willingness to develop and implement digital security practices that address organizational and/or personal risks. Changes to awareness and knowledge must also be accompanied by a willingness to institute operational changes, so that organizations can build sustainable, resilient digitally secure systems and processes.

Digital Security Framework as a Cycle

Digital security is not a goal but a process; achieving a digitally secure future is never the outcome because it is unattainable. The long-run outcome of digital security programming is instead digital security **resilience**, which refers to changes in organizational systems and culture that are contextually specific, adaptive, holistic, and sustainable. Demonstrating digital security resilience is a challenge because 1) it is difficult to document the process by which increased security know-how encourages more secure behaviors online, and 2) it is difficult to document and aggregate individual decision-making as a reflection of organizational change in digital security practices.

Measuring Digital Security Outcomes

Does your program aim to increase digital security awareness, knowledge, or adoption?



Awareness

Believes that digital threats pose a legitimate risk to organization and personal safety

Knowledge

Understands different digital security threats and appropriate interventions to mitigate those risks

Adoption

Develops and implements digital security practices that address organizational and/or personal risks

Digital security awareness, knowledge, and adoption effectively create a feedback loop, and when measured and assessed consistently over time, that data can promote learning and digital resiliency within an organization; however, the constant vigilance required is difficult to maintain. External and internal challenges can undermine an organization's digital health and resilience potential, reinforcing digital security as a cycle rather than a destination.

*There are **common barriers** to implementing digital security support activities. HROs:*

1. *Work in ever evolving threat environments.*
2. *Lack access to high-quality IT support, be it absent entirely or unaffordable.*
3. *Are often highly vulnerable and may be slow to trust implementing partners or digital security experts.*
4. *Prioritize their core function, sometimes at the expense of operational, digital security.*
5. *Include staff with uneven understanding of and appreciation for digital security.*

Digital Security Framework

	Activities	Outputs	Outcomes
Emergency Intervention	1. Provide rapid response grant for digital security materials 2. Access to digital security emergency response hotline 3. Conduct diagnostic consultation to raise awareness 4. Conduct low-lift tool use workshop	• Immediate digital security incident is addressed. • Targeted digital security resources and tools are available to staff. • HROs/HRDs are trained on specific digital security threats and on adopting specific mitigation tools.	• Staff have **increased awareness** of the severity of specific threats, targeted tools to address threats, and existing support mechanisms.
Short-term Intervention	5. Conduct targeted tool use and threat assessment workshops 6. Provide mentorship to address specific threats 7. Provide low-lift organizational policy tools, i.e., templates	• HROs/HRDs are broadly trained on basic digital security tools and practices. • HROs/HRDs are mentored on specific digital security threats.	• Staff have **increased knowledge** of actual digital security threats and mitigation and prevention tactics. • Staff **begin to adopt** digital security practices.
Long-term Intervention	8. Provide repeat,updated trainings and workshops as needed 9. Draft organization-specific digital security policies and processes 10. Provide mentorship for building digital security organizational culture	• Targeted digital security policies and processes are created. • HROs/HRDs are mentored on how to sustain a digital security culture.	• Staff **implement** digital security policies/protocols. • Staff **adopt** digital security practices. • HROs have **increased capacity** in both preventative and responsive digital security approaches.

Indicators:

- *# emergency requests responded to*
- *#HROs/#HRDs trained*
- *Reflections from HROs*
- *Change in perceived digital risk (score may go down)*
- *Change in pre/post/ex-post scores for trainings*
- *Change in OCA score*
- *Digital security trainer reflections; trainee reflections*
- *Change in risk reduction plan and/or related policy*

Freedom House

Freedom House is a nonprofit, nonpartisan organization that works to create a world where all are free. We inform the world about threats to freedom, mobilize global action, and support democracy's defenders.

1850 M Street NW, 11th Floor
Washington, DC 20036

freedomhouse.org
facebook.com/FreedomHouseDC
@FreedomHouse
info@freedomhouse.org
202.296.5101

Internews
Local voices. Global change.

Internews is an international media support nonprofit that believes everyone deserves trustworthy news and information to make informed decisions about their lives and hold power to account. We train journalists and digital rights activists, tackle disinformation, and offer business expertise to help media outlets become financially sustainable. We do all this in partnership with local communities — who are the people best placed to know what works.

2000 M Street NW, Suite 850
Washington, DC 20036

www.internews.org
facebook.com/internews
@internews
202.833.5740