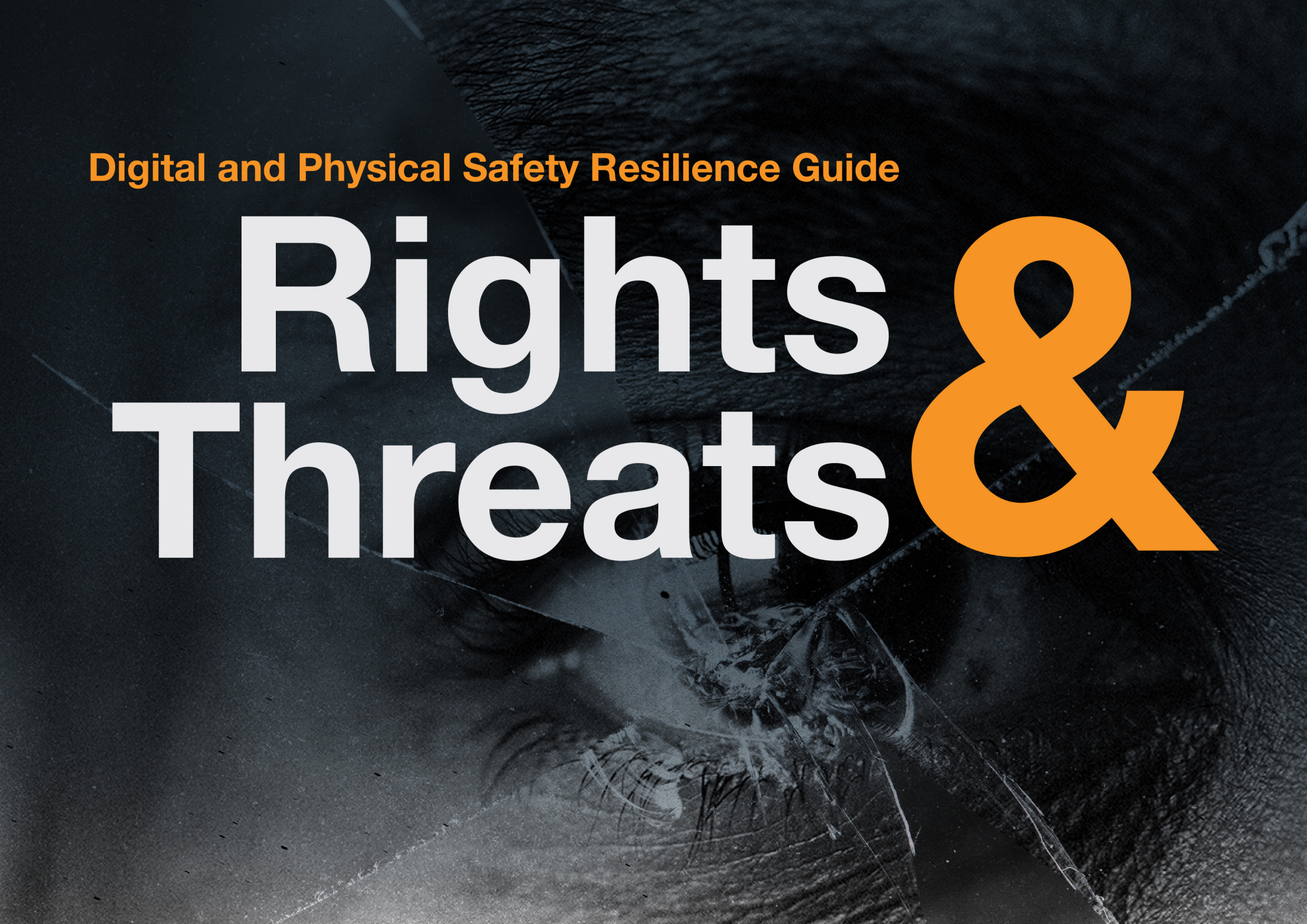

Digital and Physical Safety Resilience Guide
Rights & Threats

Digital and Physical Safety Resilience Guide

Authors: Marshal Ruhinda, Bob Bwana, Gloria Mutyaba, and Moses Karis

2025

Contents

Purpose of the Safety and Security guide:

This Digital and physical security and resilience guide is to provide guidance to gender and sexual minority groups in Uganda on how to safeguard their Information Communication Technology (ICT) assets and infrastructure. Additionally, the guide outlines measures to protect against digital and physical threats and risks targeting them and their organizations. Its specific objectives are:

- To minimize the likelihood of risks materializing, by strengthening the capacity of gender and sexual minorities to address threats and close existing security gaps.
- To minimize the impact or harm of risks through contingency plans, in case they materialize.

Contextual Background Information About the guide.

There are more than 100 organizations (registered and not registered) in Uganda that work on the rights of gender and sexual minority communities. Most of the work of these organizations revolves around research and policy advocacy, access to services, capacity development, and empowerment. These organizations also focus on community engagement, protection, and mental health of the community.

Whereas Uganda's Constitution does not expressly include sexual minority groups as one of the communities protected from discrimination, the United Nations Human Rights Committee has clarified that the term 'sex' in Article 2(1) of the International Covenant on Civil and Political Rights (ICCPR) encompasses sexual orientation. The Anti-homosexuality Act first introduced in 2014 (later annulled and then reintroduced in 2023 with amendments), already limits the rights of gender and sexual minorities and further marginalizes them. It also criminalizes any work by individuals or organizations looking to protect and promote Sexual Orientation, Gender Identity, and Gender Expression/ Characteristics (SOGIE) rights in Uganda. Furthermore, there has been an increase in threats and attacks against individuals who are perceived or known to be homosexual and or "promoting" homosexuality. These threats and attacks have been mostly instigated online including trolling, harassment, doxing, blackmail, and extortion.

Despite existing legal and policy frameworks, gender activists in Uganda continue to face significant risks and challenges.[1] Women and youth activists who work in insecure and culturally conservative contexts are at risk of

1 Behr, D.M., Groussard, H, Khaitina, V., and Shen, L. (2023). Women's Land Rights in Sub-Saharan Africa: Where do we Stand in Practice? Global Indicators Briefs No. 23. https://documents1.worldbank.org/curated/en/099432211092367495/pdf/IDU0afeba6800588804d2a0ad290368a53e64004.pdf

experiencing harassment, threats, and violence, both online and offline.[2] Particularly if they advocate for gender inequality and campaign for the recognition and respect of the rights of gender and sexual minorities in society. This can result in threats either to themselves or to the people they work with.

Owing to this challenging context, Icebreakers Uganda, Freedom & Roam Uganda and the Tranz Network Uganda developed this digital and physical resilience guide to guide gender and sexual minorities on how to sustainably engage in their work and advocacy while minimizing the potential risks and harm that may come their way, especially in digital spaces.

Personas of the Lived Experiences of Sexual and Gender Minorities in Uganda

Personas are research-driven, fictional profiles of specific user groups or individuals created to reflect their needs, behaviors, challenges, and motivations. Personas allow wider social, economic, and cultural issues to be recognized. The personas presented here aim to provide an understanding of the experiences and needs of LGBTQI+ individuals since the implementation of the Anti-Homosexuality Act (AHA) 2023. These personas were co-created in a participatory workshop with LGBTQI+ individuals in Uganda.

These personas reflect the realities of technology-facilitated gender-based violence (TFGBV) in Uganda, where LGBTQI+ individuals face doxing, blackmail, cyber harassment, outing, and economic sabotage. Their experiences highlight the urgent need for digital safety education, stronger online privacy measures, and protective mechanisms for LGBTQI+ people in hostile environments.

Through the identification of the needs, behaviors, and coping mechanisms of LGBTQI+ individuals, tailored interventions, tools and policies will be developed that empower them to navigate the challenges they encounter both online and offline.

2 United Nations (2018). The impact of online violence on women human rights defenders and women's organisations Online Misogyny. https://www.ohchr.org/en/statements/2018/06/impact-online-violence-women-human-rights-defenders-and-womens-organisations

Personas of the Lived Experiences of Sexual & Gender Minorities in Uganda

Personas are research-driven, fictional profiles of specific user groups or individuals created to reflect their needs, behaviors, challenges, and motivations. Personas allow wider social, economic, and cultural issues to be recognized. The personas presented here aim to provide an understanding of the experiences and needs of LGBTQI+ individuals since the implementation of the Anti-Homosexuality Act (AHA) 2023. These personas were co-created in a participatory workshop with LGBTQI+ individuals in Uganda.

These personas reflect the realities of technology-facilitated gender-based violence (TFGBV) in Uganda, where LGBTQI+ individuals face doxing, blackmail, cyber harassment, outing, and economic sabotage. Their experiences highlight the urgent need for digital safety education, stronger online privacy measures, and protective mechanisms for LGBTQI+ people in hostile environments.

Through the identification of the needs, behaviors, and coping mechanisms of LGBTQI+ individuals, tailored interventions, tools and policies will be developed that empower them to navigate the challenges they encounter both online and offline.

Persona 1:

Alex || 28 years old || Gay Man || IT Specialist || Kampala, Uganda

Background: Alex is a tech-savvy IT specialist working for a private company in Kampala. He is discreet about his sexuality due to Uganda's anti-LGBTQI+ laws and societal stigma. Alex uses dating apps like Grindr to connect with other gay men but is cautious about sharing personal information.

Incident: Alex was blackmailed by someone he met on Grindr. After exchanging intimate photos, the person threatened to expose Alex's sexuality to his employer and family unless he paid a large sum of money. The blackmailer also shared Alex's photos in a WhatsApp group for LGBTQI+ individuals, leading to further harassment.

Impact: Alex lives in constant fear of being outed. He has become paranoid about using dating apps and social media, limiting his interactions to encrypted messaging apps. The stress has affected his work performance, and he struggles with anxiety and depression.

Response: Alex sought help from an LGBTQI+ organization that provided digital security training. He has since deleted his dating profiles and uses a VPN to protect his online activities. He is also attending counseling sessions to cope with the trauma.

Persona 2:

Sam || 24 years old || Transgender Man || Student & Part-time Activist || Jinja, Uganda

Background: Sam is a university student studying sociology. He is an active member of a transgender support group and uses social media to advocate for transgender rights. However, he keeps his activism discreet to avoid drawing attention.

Incident: Sam's Facebook account was hacked, and the hacker posted his pre-transition photos alongside derogatory comments about his gender identity. The posts were shared widely, leading to harassment from classmates and strangers online.

Impact: Sam faced bullying at university, with peers mocking him and questioning his gender identity. He became isolated and struggled to focus on his studies. The harassment also made him fear for his safety, as he worried about being targeted by anti-LGBTQI+ groups.

Response: Sam reported the incident to Facebook and sought help from a local LGBTQI+ organization. He has since strengthened his online security and uses pseudonyms for his activism. Sam is also considering transferring to a different university to escape the harassment.

Persona 3:

Naomi || 30 years old || Transgender Woman || Hairdresser || Mbarara, Uganda

Background: Naomi is a hairdresser who runs a small salon in Mbarara. She is open about her gender identity within her close circle but remains discreet in public. Naomi uses social media to connect with other transgender women and share her work.

Incident: A client secretly recorded Naomi in her salon and shared the video on TikTok, mocking her gender identity. The video went viral, leading to online harassment and threats. Some customers stopped visiting her salon, affecting her income.

Impact: Naomi faced discrimination and lost many clients, forcing her to close her salon temporarily. She also received threatening messages from strangers, making her fear for her safety. The incident left her feeling isolated and depressed.

Response: Naomi sought support from a transgender rights organization, which helped her report the video to TikTok and provided counseling. She has since reopened her salon in a different location and uses social media more cautiously.

Persona 4:

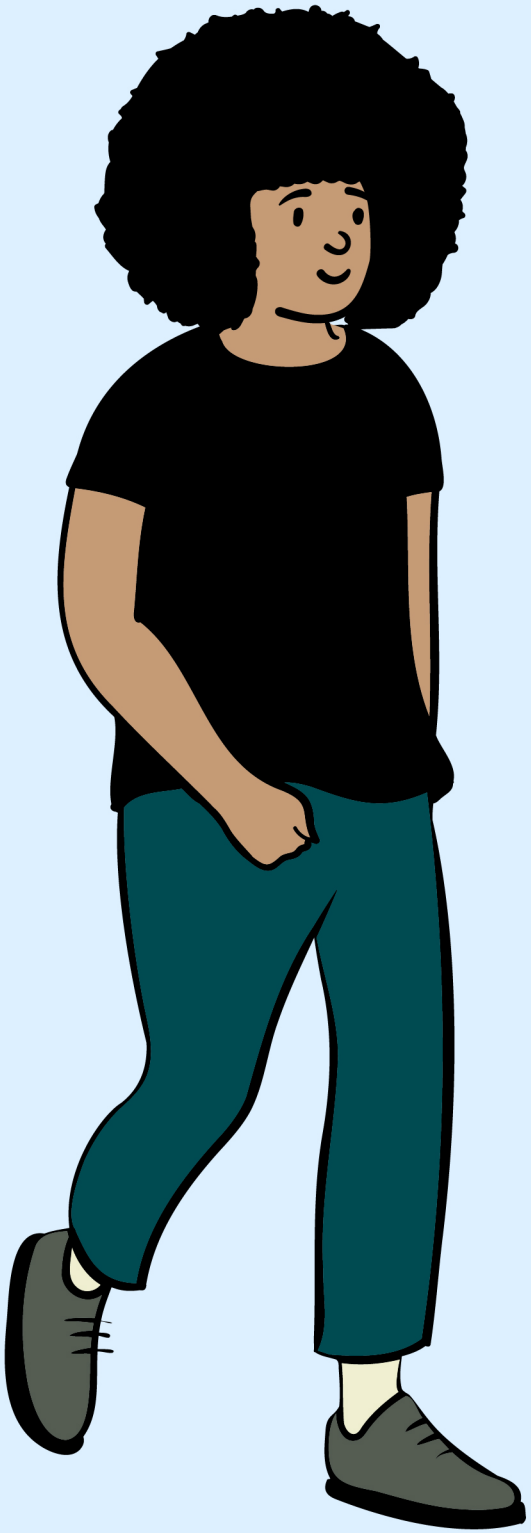
Grace || 26 years old || Lesbian || Nurse || Gulu, Uganda

Background: Grace is a nurse working at a local hospital. She is in a secret relationship with another woman and uses social media to connect with the LGBTQI+ community. Grace is careful about her online presence, using pseudonyms to protect her identity.

Incident: Grace's ex-partner, who was angry about their breakup, threatened to expose her sexuality to her colleagues and family. The ex-partner shared screenshots of their private conversations in a WhatsApp group, leading to rumors and harassment at work.

Impact: Grace faced discrimination at work, with some colleagues avoiding her and others making derogatory comments. She also received threatening messages from strangers online. The stress affected her mental health, and she struggled to perform her duties.

Response: Grace sought help from an LGBTQI+ organization, which provided legal advice and counseling. She has since limited her social media use and uses encrypted apps to communicate with trusted friends. Grace is also considering relocating to a different hospital.



Persona 5:

Linda || 29 years || Bisexual Woman || Journalist || Entebbe, Uganda

Background: Linda is a journalist who writes about social issues. She is married to a man but has a secret relationship with a woman. Linda uses social media to promote her work but is cautious about sharing personal information.

Incident: Linda's Twitter account was hacked, and the hacker posted explicit messages accusing her of being bisexual. The posts were shared widely, leading to online harassment and threats. Linda's husband also saw the posts, causing tension in their marriage.

Impact: Linda faced backlash from her colleagues and the public, with some accusing her of promoting immorality. The incident also strained her relationship with her husband, who questioned her loyalty. Linda struggled with anxiety and guilt, affecting her work and personal life.

Response: Linda sought help from a digital security expert and an LGBTQI+ organization. She has since secured her social media accounts and uses pseudonyms for her activism. Linda is also attending couples counseling to repair her relationship with her husband.

Persona 6:

David || 32 years || Bisexual Man || E-commerce Entrepreneur || Fort Portal, Uganda

Background: David runs an online business and uses social media to market his products. He has dated both men and women but remains discreet about his bisexuality due to Uganda's hostile environment. He mostly engages in LGBTQI+ discussions through Telegram and private Twitter spaces.

Incident: An ex-boyfriend, feeling betrayed after David started dating a woman, retaliated by exposing their private messages and photos on Facebook, and tagging his business page. He also falsely accused David of being HIV-positive to tarnish his reputation. Customers and business partners began questioning David's credibility, leading to a significant drop in sales and online abuse from strangers.

Impact: David's business suffered financially as clients withdrew support. He faced public humiliation, and family members confronted him about his sexuality. He developed severe anxiety and struggled to maintain his livelihood.

Response: With guidance from an LGBTQI+ advocacy group, David issued a takedown request for the harmful content. He also changed his business branding and switched to selling on anonymous online platforms. He now limits his online interactions and prioritizes secure communication methods.

Persona 7:

Riley || 25 years || Nonbinary (They/Them) || Graphic Designer & Freelancer || Jinja, Uganda

Background: Riley identifies as nonbinary and works remotely as a freelance graphic designer. They are vocal about gender diversity on social media and contribute to online LGBTQI+ advocacy spaces. They dress androgynously and often face discrimination in public.

Incident: A conservative influencer targeted Riley after they posted about gender identity on TikTok. The influencer's followers flooded Riley's account with hate comments, misgendering them and calling for violence against Western LGBTQ+ ideology. Riley's profile was mass-reported, leading to TikTok suspending their account. Their personal phone number was also leaked, resulting in harassing calls and threats.

Impact: Riley suffered from cyberbullying and struggled with emotional distress. They lost freelance clients who feared backlash from being associated with LGBTQI+ activism. The stress and fear made Riley temporarily relocate to stay with a trusted friend.

Response: Riley received support from a digital rights group that helped them restore their social media accounts and improve security settings. They also changed their phone number and used aliases for advocacy work. They continue to work remotely but limit their online presence to avoid further attacks.

Scope of the guide

This guide is designed for gender and sexual minority individuals and rights practitioners operating in Uganda, as well as organizations and service providers addressing issues affecting the gender and sexual minority community. In Uganda's current socio-political context, individuals and community practitioners need to prioritize their safety, the well-being of their beneficiaries, the security of program-related information, the integrity of their partnerships, and the protection of their reputations.

Approach to Risk Management:

This guide combines the following risk management strategies:

1. Acceptance strategies aimed at gaining the support of allies and stakeholders
2. Deterrence measures to prevent unwanted access, and a collective approach that leverages external strengths and capacities for collective security.

Roles and Responsibilities

LGBTQI+ Individuals

All LGBTQI+ individuals may collaborate with their leaders to achieve the objectives outlined in this guide. Each individual may implement the digital security measures specified in this guide and adhere to its guidelines as well as other relevant documents and frameworks. Individuals are expected to report any observed or encountered online and physical security incidents and safeguard information and access entrusted to them by their community leaders.

Community Leaders

Community Leaders at all levels hold the overall responsibility for the safety and security of the organization and community, including the welfare of all staff and community members. Community Leaders are tasked with ensuring the communities and organization's compliance with this guide and may delegate specific responsibilities to staff and community representatives who will monitor and provide regular updates on compliance.

In collaboration with other leaders, they are responsible for anticipating, analyzing, and identifying potential risks associated with public statements, and organizational and community online and social media activity. They must review posts and documents before publication to prevent damaging the organization and community's reputation and mitigate any other risks that could happen to any section of the community from such publications.

In collaboration with the Head of Finance/Administration/Grants/Fundraising, organizations are responsible for planning and allocating resources for items in the guide that require funding. If specific items lack the necessary funds this person should take the lead in coordinating efforts to secure the required resources.

The security focal person, the ICT team, and senior management of community organizations will ensure compliance with this guide through various methods including but not limited to feedback from members, internal audits, and external audits.

The guide

It highlights potential risks, and associated vulnerabilities offering preventive strategies and contingency responses in case these risks materialize. As a living document, it requires regular updates to reflect changes in the Ugandan context and the evolving work of community activists.

We highly recommend and encourage community leaders and organizations to adhere to the recommendations in this guide to protect against digital and physical threats and risks to the community.

Doxing: The act of publicly revealing or publishing private, personal, or sensitive information about an individual or organization without their consent, typically with malicious intent.

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Accessing Public Wi-Fi Without Proper Security Measures exposes users to risks such as interception of login credentials, unauthorized access to accounts, or data theft. • Low Awareness of Digital Threats and Online Security Risks makes individuals more susceptible to inadvertently revealing personal or sensitive information. • Oversharing personal sensitive information online creates a public record that malicious actors can use to track, target, or harass individuals. • Relying on insecure messaging platforms without end-to-end encryption allows attackers to intercept communications and access private conversations.	• Use pseudonyms or usernames that don't reveal your real name or identity. • Delete addresses, workplaces, and location tags from your accounts. • Set posts to "friends only" and limit who can view your profile. • Don't share details like your address, phone number, or workplace in posts or messages. • Use a VPN and disable public network sharing when using public Wi-Fi. • Use strong, unique passwords and enable two-factor authentication (2FA) on all accounts. • Avoid using the same username across multiple platforms. • Use a unique email address dedicated to sensitive contacts or financial accounts. • Regularly check for and request the removal of your data from websites and data brokers.	• Take screenshots, record URLs, and save timestamps of where your personal information has been shared. • Immediately report the doxxing incident to the platforms or websites hosting the information. • Contact a lawyer or a legal aid organization specializing in digital rights or privacy to understand your options and file a formal complaint if necessary. • Inform close friends, family, or colleagues about the incident so they can be cautious of potential impersonation or phishing attempts. • Change passwords for your online accounts, enable two-factor authentication, and review account activity for any unauthorized access. • Reach out to organizations or advocacy groups that support LGBTQI+ individuals for advice, resources, and emotional support.

Trolling: the act of deliberately posting provocative, offensive, or disruptive messages online with the intent to elicit emotional reactions, create conflict, or derail discussions.

Cyberbullying: the use of digital platforms to harass, intimidate, or harm an individual repeatedly.

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Ignorance of digital rights and legal protections against online abuse. • Limited understanding of how online attacks (e.g., trolling, phishing, or hate campaigns) occur leaves individuals vulnerable. • Posting personal details like your location, contacts, or affiliations can make you a target for cyberbullying. • Working on sensitive and socially controversial topics like LGBTQI+ rights, feminism, or politics can attract targeted harassment.	• Limit your online interactions to trusted friends and contacts to reduce exposure to trolls. • Disable or limit comments on sensitive posts, or use moderation tools to filter harmful messages. • Develop a clear strategy for handling trolls, including when to ignore, block, or report them. • Immediately block trolls and use platform reporting tools to flag abusive accounts or content. • Use tools like word filters to block harmful language or set rules for who can tag or message you. • Don't respond to hateful or provocative comments, as this can escalate the situation. • Regularly update passwords, enable two-factor authentication, and monitor account activity to prevent breaches. • Be cautious when posting about sensitive or controversial topics; use discretion to avoid unnecessary exposure.	• Avoid replying to hateful comments or messages. Engaging often encourages further harassment. • Use platform tools to block trolls, preventing them from interacting with or viewing your content. • Report harmful posts or accounts to the platform, citing its policies on harassment and abusive behavior. • Turn off notifications or use focus modes to reduce exposure to hateful messages, especially during rest periods. • Take screenshots and save evidence of trolling or cyberbullying for future reporting or legal action. • Reach out to friends, family, or trusted networks for emotional support and advice. If needed, contact a counseling service for professional help. • If the trolling escalates, seek guidance from organizations that specialize in online safety and advocacy for targeted groups

Hacking refers to the unauthorized access, manipulation, or control of computer systems, networks, or devices.

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Many people don't know how to protect their devices and accounts from cyber threats. • Limited understanding of tactics like ransomware, phishing, social engineering, or deepfakes makes individuals easy targets. • Clicking suspicious links or downloading unknown files out of curiosity can compromise your security.	• Create unique, complex passwords for each account and avoid reusing them. • Add an extra layer of security by using multi-factor authentication for all your accounts. • Protect your data by using an authentic VPN when browsing on public or unprotected networks. • Only install apps from official app stores like Google Play or the Apple App Store. • Regularly update apps to fix security vulnerabilities and remove old or unused ones. • Don't open links or attachments from unknown sources, even if they look legitimate. • Keep your devices locked with passwords or biometrics and never leave them unattended.	• Learn how to lock or erase your device remotely to protect sensitive information. • Regularly back up your data so you can quickly recover important files if hacked. • Inform your trusted contacts and your organization's digital and data security team immediately to help manage the situation. • Update all passwords for compromised accounts and enable multi-factor authentication. • Report the hacking to the platform, service provider, or relevant authority for further action. • Run a full antivirus or anti-malware scan on your devices to identify and remove threats.

Physical trailing refers to the act of following or monitoring an individual in the real world, usually in a covert or secretive manner, in order to observe their activities, movements, or interactions.

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Failing to use a VPN leaves your location data vulnerable to tracking. • Limited knowledge of how to spot or monitor if someone is following you. • Absence of a clear plan to follow in case you are physically trailed.	• Vary your daily routes and routines to make it harder for anyone to track you. • Ensure all staff receive basic security training within their first three weeks at the organization. • Always remain alert and observe for unusual behavior or vehicles around you. • Rely on trusted drivers or transport services to minimize risks. • Only share your routes and destinations with trusted individuals.	• Immediately inform your designated security contact about the situation. • Head to the nearest police station or a crowded, secure public place. Observe the follower's behavior carefully. • Take note of the person's appearance, clothing, vehicle, license plate, and any other identifying details. • Do not engage or confront the trailer; focus on getting to safety. • If you feel unsafe, call a trusted friend, colleague, or authority to join you.

Online Surveillance: Online surveillance refers to the monitoring, collection, and analysis of individuals' online activities, behaviors, and personal information, often by governments, corporations, or other organizations.

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Limited or inconsistent use of VPN for securing online activities. • Accessing sensitive accounts over public Wi-Fi without using secure connections. • Limited awareness of phishing attacks that could compromise sensitive data. • Using unregistered or outdated anti-virus software that doesn't provide proper protection. • Posting sensitive or identifiable information online that can be exploited for surveillance. • Using messaging apps like WhatsApp may not provide the highest level of security for sensitive communications.	• Regularly update the operating system and anti-virus software on both work and personal devices to guard against security threats. • Avoid sharing sensitive personal information or your location on social media or online platforms to reduce the risk of being tracked.	• Immediately block any compromised online accounts to prevent further surveillance or unauthorized access. • Quickly update all device software and anti-virus programs to patch vulnerabilities and protect against further threats.

Phishing: Phishing is a form of social engineering where attackers deceive individuals into revealing sensitive information such as usernames, passwords, or credit card details.

Malware Attacks: Malware (short for malicious software) refers to any software intentionally designed to harm or exploit a computer, network, or device.

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Lack of understanding of how phishing and malware attacks work. • Failure to install or update registered antivirus software leaves systems exposed to malware and malicious attacks.	• Use separate accounts for personal and work activities to protect confidential information. Admin rights should be restricted. • Ensure device operating systems are regularly updated by the manufacturer to patch vulnerabilities. • Install and maintain up-to-date antivirus software to detect and prevent malware attacks. • Enable automatic updates for both the operating system and software to protect against known threats. • Run regular malware scans on all devices to detect and remove threats. • Conduct periodic training to help staff recognize and avoid phishing and malware risks. • Avoid connecting unfamiliar or unverified portable devices to reduce the risk of malware transfer.	• Immediately inform all relevant contacts about the compromised account to prevent further damage. • Update passwords for compromised accounts and any other accounts that share the same credentials. • Block or suspend the compromised accounts to prevent unauthorized access while you investigate and resolve the issue.

Data Breach / Loss: Refers to an incident where sensitive or confidential information is accessed, disclosed, or destroyed without authorization.

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Not always using Tresorit or other secure cloud services for storing sensitive files. • Failing to encrypt sensitive files before storing or sharing them.	• Always set strong passwords. Avoid using weak methods like patterns or pins. • Ensure devices automatically lock after a period of inactivity. • Use encrypted email and secure phone lines for sensitive communication. • Back up important data regularly to a secure off-site location.	• If possible, remotely erase compromised data from affected devices to prevent further exposure. • Access secure backup storage to restore lost or compromised information, ensuring no data is permanently lost.

Harassment and Intimidation

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Ignorance of relevant laws and protections can increase vulnerability to harassment. • Living an extravagant lifestyle can attract negative attention or feed into harmful stereotypes about the LGBTQI+ community. • Not being aware of or using digital security tools can expose individuals to online harassment. • Engaging in community work can make individuals more visible and vulnerable to harassment due to its controversial nature. • Not being ready to handle harassment or intimidation can escalate situations and increase emotional strain. • Breaching confidentiality within the community can lead to increased targeting and vulnerability to harassment.	• Understand the legal protections against harassment and intimidation to know your rights. • Avoid engaging with unfamiliar people, whether online or offline, to reduce exposure to potential harm. • Ensure staff are familiar with the organization's vision, mission, and values to stay grounded in its protective framework. • Always work with a colleague or team when going on missions to ensure safety and support. • Each staff member must have and stick to a personal security plan for protection in risky situations.	• Do not engage in physical or verbal fights. Stay calm and try to avoid reacting to the intimidation. • If the situation turns violent, safely leave the area when possible. • Notify the organization's security focal person immediately about the incident. • Evaluate the situation, and take appropriate action based on the risk level. • Seek help from legal, community, social, or medical/mental health support networks if necessary.

Physical Assault and Abuse (e.g. corrective rape)

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Increased risk when moving without companions, especially in unsafe areas. • Certain clothing or appearance may attract unwanted attention or trigger hostility. • Living in areas known for hostility or discrimination increases vulnerability. • Engaging in work related to marginalized communities may expose individuals to targeted violence. • Not knowing how to defuse potentially dangerous situations can escalate tensions. • Failing to analyze and mitigate risks linked to sensitive or controversial work increases the danger.	• Whenever possible, move with a companion or in a group for added safety. • Keep a trusted contact informed of your whereabouts at all times. • Gain basic physical defense skills to protect yourself in dangerous situations. • Wear clothing that minimizes attention or scrutiny. • Do not engage directly with potential perpetrators to reduce risk. • Always assess the situation carefully and rely on your judgment to make decisions. • Avoid responding to unknown phone calls, texts, or messages that may be from malicious sources.	• Get to a safer location as soon as possible. • If safe, report the incident to the nearest police station immediately. • Fight back only if you believe you can successfully defend yourself. • Block unknown phone callers and suspicious requests on social media. • Reach out to your designated legal support (para-legal) for assistance.

Arbitrary Arrest and Extortion

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Limited knowledge of rights and relevant laws. • Tendency to comply with extorters' demands without seeking advice. • Extravagant lifestyles that attract unwanted attention. • Activities and advocacy efforts linked to marginalized communities increase risk. • Threats of leaking sensitive personal or organizational information. • Inadequate online and offline personal security measures. • No risk assessment or analysis for high-stakes activities and programs. • Absence of clear guidelines for staff involvement in sensitive client cases.	• Use digital security measures like encryption and strong passwords to secure sensitive data. • Ensure all staff and partners understand the importance of confidentiality and adhere to it. • Transfer risk by outsourcing or involving trusted third parties in high-risk activities when necessary. • Provide training on legal rights, laws, and protections to all staff and stakeholders.	• Remain calm and avoid resisting arrest or confrontation. Try to establish a friendly rapport with officers, if possible. • Ask to see the arrest warrant if applicable. • Request permission to inform trusted individuals of your arrest. • Insist on having your lawyer or paralegal present before answering any questions or providing information. • Remain silent except for necessary safety-related communication. • Mentally note the events, questions, and any interactions for future reference. • Ask for essential items, like medication, food, or a change of clothes, if detained. • Designate a community leader to notify key stakeholders and partners. • Your lawyer or paralegal should advise on the best response strategy, and leadership will make the final decision. • Call for backup from your paralegal or legal support team if needed.

Organization Office Break-In / Office raid / search by law enforcement agencies

Related Vulnerabilities	Standard Operating Procedures (How to prevent)	Contingency (emergency response)
• Some staff may not know how to respond appropriately during a raid. • Limited knowledge of techniques to calmly handle tense situations. • The nature of the work may attract scrutiny or misunderstanding. • Having a visible office location increases exposure to raids. • Issues with registration status can be used against the organization. • Delays in filing returns or meeting legal obligations may trigger raids.	• Train all staff in basic security guides within the first three weeks of joining. • Keep doors locked during and after work hours to limit unauthorized access. • Restrict visitors to essential appointments and maintain a visitor logbook. • Avoid sharing the office location and other sensitive information online or offline. • Remove LGBTQI+ identifying information like logos, colors, and contact details from public platforms. • Maintain proper registration, file tax returns on time, and fulfill all legal obligations. • Establish connections with state officials and NGO administrators to navigate risks effectively.	• Avoid resistance or confrontation during the search process. • Designated staff must call the organization's lawyer immediately. • Politely ask to see the search warrant and document the officer in charge's name and details. • Seek permission to observe the search to prevent tampering, planting of evidence, or loss of items. • Store sensitive information in password-protected files or containers if possible during the search. • Compile a detailed list of all items seized by the officers. • Obtain clear information about the reasons for the raid and the organization's operational future. • Inform the Board, senior management, and key stakeholders immediately. • Draft a strategy to address the raid's impact and mitigate harm to stakeholders. • Management must update all staff on the situation and outline the next steps clearly.

Annex

Here are additional resources for further information and learning.

1. **Stand Up Manual:** https://defenddefenders.org/wp-content/uploads/2023/04/STAND-UP-MANUAL-23122022-2-1-1.pdf
2. **New Protection Manual:** https://www.protectioninternational.org/wp-content/uploads/2022/12/New-protection-manual-English.pdf
3. **Guide:** https://elibrary.defenderscoalition.org/reports/Safety%20and%20Protection%20Guide%207-17-2018%20small.pdf
4. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
5. https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses
6. https://www.kaspersky.com/resource-center/preemptive-safety/small-business-cyber-security
7. https://www.protectioninternational.org/wp-content/uploads/2022/12/New-protection-manual-English.pdf
8. https://www.lenels2.com/en/news/insights/the-ultimate-guide-to-physical-security.html
9. https://digitalsafetea.com/
10. https://chooseyourownfakenews.com/

Security Incident Reporting Template

SECURITY INCIDENT REPORT FORM

Name of person reporting:	
Date of security incident:	
Location of the incident:	
Time and duration:	
Person/people involved:	
Description of the incident:	

SRT HUMAN RIGHTS VIOLATIONS TEMPLATE

ORGANIZATION:

Reporting Period:

N/S	Particulars	Type of violation (This should be as detailed as possible)	Date(s) & place	Perpetrator(s)	Action Taken (Nature of support extended, who supported)	Nature of evidence available /source of information	Verification details
1	Name: Age: Contact: Sexual orientation: Gender identity:		Date of violation: Place of violation: When was the violation reported?				Who verified? Contact of the person that verified: Verification details