VITAL VOICES
GLOBAL PARTNERSHIP

DIGITAL SAFETY PLAN
FOR WOMEN LEADERS

This toolkit was developed by Vital Voices Global Partnership in collaboration with Safe Sisters, Internews.

Please do not distribute without written permission from the Vital Voices Crisis Response Team, crisis@vitalvoices.org.

Crisis Readiness Training 2024, Morocco

PLAN CONSIDERATIONS

Now that you have gone through the entirety of the Crisis Readiness Toolkit, it is time to apply your learnings to a safety plan. Identify an incident, consider the details, and expand upon the following prompts to create a detailed safety plan.

How to use this tool: Women leaders facing crises should use this tool to plan for how to prepare and respond to potential threats to their safety. Leaders should create a security plan for each individual incident/ threat they are facing.

INCIDENT

Examples: Arrest, Natural Disaster, Online Threat

Data Breach

LIKELIHOOD

High, Medium, Low

Medium

IMPACT

High, Medium, Low; Individual, Team, Organization Impact
**Refer to Risk Assessment in Toolkit*

High

WARNING SIGNS

Signs you might be in danger
Tip: *Think through scenarios with others, like your team, if a sign occurs what action will we take?*

Unusual login attempts, unauthorized access alerts, unexpected data transfers

RESOURCES

Consider resources you either currently have or need in order to action your plan below. These resources could be training, funding, capabilities or skills.

	RESOURCES I HAVE	RESOURCES I NEED
1	**Examples:** IT Security team, Access to cybersecurity tools (VPN, firewalls), regular security training programs	**Examples:** Advanced threat detection software, Additional cybersecurity training for staff, Budget for cybersecurity enhancements
2		
3		
4		

TRUSTED CONTACTS

Think of dependable people or organizations upon whom you can call during an emergency.

	CONTACT	CONSIDERATIONS
1	**Examples:** IT Security manager, External cybersecurity consultant, Legal advisor	[Mobile: Insert here] [E-mail: Insert here] [Signal/Whatsapp: Insert here]
2		
3		
4		

ACTION PLAN

Expanding Your Safety Plan

Fill this out with actions you need to take to prepare yourself for potential incidents and respond if they occur. Consider the timeline for each action, as well as considerations. Mark off actions as you complete them.

READY:

Actions to take prior to an incident occurring

	ACTION	STATUS	TIMELINE	CONSIDERATIONS
1	Procure digital safety detection software	Select from the following	Immediate	Review FrontLine Defenders' list of recommendations
2	Set up real-time alerts for unusual login attempts and unauthorized access	Select from the following	Quarterly	Regularly test systems
3	Ensure multi-factor authentication (MFA) is enabled on all devices and conduct regular checks	Select from the following	Weekly	Identify team member responsible for enforcing MFA
4	Provide step-by-step guides for MFA and conduct regular audits to ensure staff is aware of guidelines	Select from the following	Immediate	Ensure guides are clear and easily accessible for staff
5	Review and update alerts based on new information of threats	Select from the following	Immediate	Stay informed about the latest security threats and adjust alerts accordingly
6	Conduct quarterly training on cybersecurity best practices, including phishing and password management	Select from the following	Immediate	Ensure training materials are up to date with current threats. See list of resources below
7	Train employees on security best practices on basic cyber security, including phishing and password management	Select from the following	Quarterly	Make sure all employees, especially new hires, are trained regularly

Ready continuted on next page

READY (CONTINUED)

	ACTION	STATUS	TIMELINE	CONSIDERATIONS
8	Use simulated phishing attacks to test employee awareness and provide feedback to staff on areas for improvement	Select from the following	Quarterly	Provide feedback to employees based on their responses to phishing simulations
9	Schedule automated backups to a secure cloud service such as Google Drive, Microsoft SharePoint	Select from the following	Weekly	Ensure backup schedules are consistent and reliable, test recovery processes periodically

RESPOND

Actions to take once an incident occurs

	ACTION	STATUS	TIMELINE	CONSIDERATIONS
1	Disconnect affected systems from the network	Select from the following	Immediate	Have a predefined protocol and ensure all team members are familiar with it
2	Change passwords and access credentials on all main devices	Select from the following	Immediate	Use a password manager to ensure strong, unique passwords. Confirm no unauthorized changes have been made prior to updating
3	Disable compromised accounts	Select from the following	Immediate	Maintain a list of accounts with various levels of access to prioritize disabling high-risk accounts first
4	Send a detailed incident report to the IT Security team and management	Select from the following	Within 1 hour	Include key details like the breach time, affected systems, and actions taken
5	Engage cybersecurity experts to trace the breach source and assess the extent of data exposure	Select from the following	Within 24 hours	Choose experts with experience in handling similar incidents. Ensure a contract is in place for confidentiality and response

Respond continuted on next page

RESPOND (CONTINUED)

	ACTION	STATUS	TIMELINE	CONSIDERATIONS
6	Preserve all logs and evidence for potential legal action	Select from the following	Within 48 hours	Keep logs safe and ensure they are not tampered with
7	Draft and send notifications to stakeholders, including employees, clients, and partners	Select from the following	Within 48 hours	Be transparent about the breach details and outline steps being taken to mitigate risks

RECOVER

Actions to take after an incident occurs

	ACTION	STATUS	TIMELINE	CONSIDERATIONS
1	Conduct a thorough review of existing security policies and update them to address identified vulnerabilities	Select from the following	Post-incident	Involve cross-functional teams to ensure comprehensive coverage
2	Implement advanced security tools such as intrusion detection systems and protection	Select from the following	Within 1 month	Prioritize enhancements based on the severity of vulnerabilities exposed during the breach
3	Organize a debriefing session to evaluate the incident response and identify areas for improvement	Select from the following	Within 2 weeks	Document findings and update the incident response plan accordingly
4	Schedule ongoing employee training sessions focusing on lessons learned and new security protocols	Select from the following	Ongoing	Use feedback from post-incident reviews to tailor training content