Tips for Promoting Physical and Digital Security

RHNTC
REPRODUCTIVE HEALTH
NATIONAL TRAINING CENTER

Ensuring the safety and security of professionals working in sexual and reproductive health is part of effectively delivering services and programs. This resource is designed to get both Title X and Teen Pregnancy Prevention (TPP) Program grantees thinking strategically about staff safety and organizational security. When doing this work, it's recommended that project leaders collaborate with staff in relevant departments (like IT personnel and building administrators).

Safety and Security Defined

Safety: The condition of being protected from, or unlikely to cause, danger, risk, or injury.

Security: The state of being free from danger or threats.

Physical Security: The protection of the physical integrity of the organization and its members, including protection of:

- Buildings
- Hardware
- Physical files and documentation
- Staff and volunteers (including during travel, events, and workshops)

Digital and Information Security: The protection of online and offline data and infrastructure, such as websites, databases, servers, and emails. Also includes the protection of all channels of communication.

Conduct a Threat Assessment

All good safety and security planning begins with understanding the possible threats your organization faces. Invest time and resources into examining any risks, threats, and vulnerabilities to physical safety (e.g., someone gaining unauthorized access to your offices or making a threat of violence) and digital safety (e.g., hacking or online harassment).

- Prepare a list of the material resources (e.g., devices, software, websites, and servers) and human resources your organization wants to protect. While you undoubtedly want to protect all staff and volunteers, note those whose security is critical to your organization's success and longevity (e.g., key leaders or media spokespeople).
- Brainstorm a list of threats relevant to your organization and its staff (e.g., community members who disagree with your approach, mission, or work).
- Forecast the probability and potential impact of each threat as well as strategies to mitigate them.
- Update your risk matrix as your organization and the landscape changes.

Create a Security Road Map

Putting together a security policy and road map for your organization can help you be proactive while also preparing for worst-case scenarios. Change takes time and starting with small steps can help you build toward your long-term goals.

- Compile your organization's existing security approach, including infrastructure (e.g., physical or cloud storage, surveillance cameras, access controls), policies, and accounts.
- Compare your security approach against the key threats and identify what is missing.
- Identify initial security objectives, such as protecting your organization's website.
- Document potential improvements to your security approach.
- Prioritize the potential improvements and define your initial areas of focus.
- Designate certain staff members to keep documents updated.

Cultivate a Security Culture

Making security the concern of all members of your organization can help reduce your overall risk. Intentionally build awareness and accountability across your organization to foster a stronger security culture.

- Once you have established your organization's security baseline, communicate key information that will empower staff to take action and increase their awareness.
- Conduct trainings about security best practices.
- Assemble a basic checklist of security actions that staff can follow.
- Incorporate key security lessons into your workflows, including staff onboarding and offboarding.
- Proactively monitor threats and take steps to protect your staff.

Suggested Resources

Holistic Security: A Strategy Manual For Human Rights Defenders

Ford Foundation's Cybersecurity Assessment Tool (CAT)

Digital Defense Fund

Security Education Companion

SOAP (free online security policy generator)

This publication was supported by the Office of Population Affairs (Grant FPTPA006030 and Grant TPSAH000006). The views expressed do not necessarily reflect the official policies of the Department of Health and Human Services; nor does mention of trade names, commercial practices, or organizations imply endorsement by the U.S. Government.