One Society Organization for Peace and Development

(Binding policy for all employees and collaborators to protect information and people)

ONE COMMUNITY ORG
PEACE & DEVELOPMENT

Approved
30/ march, 2025

Contact us: info@ocosudan.org ☎ +249995002443 Location: Port Sudan - Sudan

Digital Security and Data Protection

Preamble

Given the nature of the Organization's work in sensitive and conflict zones, and in order to preserve the safety of staff and the privacy of beneficiaries, this policy aims to establish strict controls for the use of technology and the handling of digital data. Digital security is considered an integral part of field and personal security.

Chapter 1: Data Classification

Article 1: Data Confidentiality Levels All Organization data is classified into three levels and handled accordingly:

1. **Public Data:** Information available for public release (e.g., published annual reports, news of public activities). *Does not require encryption.*
2. **Internal Data:** Information specific to internal work, the leakage of which does not cause serious harm (e.g., project drafts, ordinary meeting minutes, administrative forms). *Requires passwords.*
3. **Confidential/Sensitive Data:** Information the disclosure of which poses a risk to the lives of individuals or the reputation of the Organization (e.g., beneficiary lists, data of violence survivors, detailed financial data, bank account passwords, and activities in sensitive areas). *Requires high-level encryption and limited access.*

Chapter 2: Device and Account Security

Article 2: Device Protection (Computers/Phones)

1. All work devices must be secured with a strong password or biometrics, with automatic screen lock enabled after **two minutes** of inactivity.
2. It is prohibited to leave work devices (laptops/phones) unattended in public places or vehicles.
3. Hard Disk Encryption (using BitLocker or FileVault) must be enabled for all portable computers containing sensitive data.

Article 3: Passwords

1. The use of weak passwords (e.g., 123456 or the Organization's name) is prohibited.
2. **Two-Factor Authentication (2FA/MFA)** must be enabled on all sensitive accounts (Organization email, Facebook, Bank Accounts). This is a mandatory clause with zero tolerance.
3. Sharing personal passwords with any colleague under any circumstances is prohibited.

Chapter 3: Communications and Correspondence Security

Article 4: Approved Communication Channels

1. The Organization adopts the **Signal** application for instant communication regarding sensitive issues and field operations, due to its encryption and auto-delete features.

2. The use of **WhatsApp** or **Messenger** to exchange "Confidential Data" (e.g., name lists, security movements) is prohibited due to the ease of hacking or metadata tracking in certain circumstances.
3. The Organization's official email is the only medium for formal correspondence with donors and partners.

Article 5: Virtual Meetings

1. When holding meetings via Zoom or Google Meet, the "Waiting Room" feature must be enabled, and the meeting link must not be shared publicly on social media.

Chapter 4: Handling Beneficiary Data

Article 6: Data Collection and Storage

1. **Informed Consent** must be obtained from the beneficiary before taking any photo or recording any personal data.
2. It is prohibited to store photos or data of vulnerable groups (children, violence victims) on employees' personal phones. Such data must be transferred immediately to the Organization's **Secure Cloud** and deleted from the phone.
3. Data collected must be minimized to the absolute necessity required for work (**Data Minimization**).

Article 7: Data Sharing Beneficiary lists may not be shared with any external entity (governmental or non-governmental) without written approval from the Executive Director, and only after verifying the data protection policies of the receiving entity.

Chapter 5: Internet and Network Usage

Article 8: Wi-Fi Networks

1. Avoid using public open Wi-Fi networks (in airports and cafes) to access the Organization's financial or administrative systems.
2. If it is necessary to use a public network, a trusted **VPN** (Virtual Private Network) must be used to encrypt the connection.

Article 9: Downloads and Software Downloading **Cracked Software** on Organization devices is prohibited, as it often contains malware and spyware.

Chapter 6: Incident Response

Article 10: Reporting Hacks In the event of a lost device, suspected account hack, or receipt of a suspicious link, the employee must:

1. Disconnect the device from the internet immediately.
2. Report to the Technical Officer or Direct Manager immediately (without delay or fear of punishment).
3. Change passwords for affected accounts from another secure device.

Article 11: Remote Wipe The Organization reserves the right to perform a **"Remote Wipe"** of data on any device belonging to it in case of theft or loss, to protect data from falling into the wrong hands.

Conclusion

Adherence to this policy is not a technical choice but a commitment to the safety of the team and beneficiaries. Any negligence in applying these controls (such as sharing passwords or neglecting software updates) is considered a major misconduct subject to accountability.

Executive Director Approval Yassin Ahmed

Effective Date 26/Dec/2025

ONE COMMUNITY ORG. ONE COMMUNITY ORGANIZATION PEACE & DEVELOPMENT