# SECURING DATA

This document is produced in order to create a reference point for front-liners when considering data security at their organisations. It highlights the importance of data protection and offer practical tools that can be applied in order to boost data protection and security.

## PRINCIPLES OF DATA SECURITY

### CONFIDENTIALITY

Ensuring that access to each piece of data is restricted to the people who truly need it in order to fulfill a known, clear and legitimate purpose.

### AVAILABILITY

Keeping data available for any legitimate access.

### RETENTION

Destroying the data where and when it is no longer needed.

### AWARENESS

Recognising the sensitivity of personal data by assessing threats to confidentiality and integrity and the associated risks to people of concern such as extortion, blackmail, torture,death, fraud, community tensions or defamation.

### INTEGRITY

Preventing data alteration during collection, storage and processing phases.

### LAWFULNESS

Enforcing Human Rights Law and and the relevant body of national and international law that protects the right to privacy and security.

### DO NO HARM

Avoiding risk by preventing any illegitimate access, alteration, loss or misuse of data.

Recognising that the tools used to collect, store, process and share data are generally not designed for humanitarian work, thus not secure enough. Hence, it is important to address the actual or possible security flaws of such tools with additional measures.

### ACCOUNTABILITY

Striving to adhere to the highest possible standards when it comes to protecting vulnerable people and their interests, in order to be accountable to the people we seek to assist and who are the rightful owners of their data, as well as partners, supporters and donors.

## WHAT DATA SHOULD WE PROTECT?

As soon as data is related to people, it is sensitive and hence must be protected.

Very powerful algorithms are now able to reconstruct or infer information that no human could ever reach, including Personal Identification Information, location and habits, by matching millions of data sets from thousands of sources, each holding billions of data pieces.

## FURTHER RESOURCES

Handbook on Data Protection in Humanitarian Action (ICRC)
Data Responsibility Guidelines (OCHA)
Data to the rescue: how humanitarian organisations use information (podcast) (OCHA)
Policy on the Protection of Personal Data of Persons of Concern to UNHCR

CAMEALEON · Caritas Lebanon · Première Urgence Aide Médicale Internationale · SOLIDARITÉS INTERNATIONAL · OCHA · UNHCR The UN Refugee Agency · Inter-Agency Coordination Lebanon

# PRACTICAL TIPS ON SECURING DATA

## HOW TO SECURELY SEND DATA?

**Data sent by email is like a postcard: very easy to intercept, and anyway visible by the mailing staff. Therefore, any data should be encrypted before being sent.**

Encrypt the file before attaching it to an email. https://www.7-zip.org is free and open-source and will do it in two clicks. MS Office 2016+ offers a reliable built-in password protection feature in the "File" menu.

Send the password to the data receiver through an end-to-end encrypted medium, like **Signal Messenger, Telegram, encrypted email** or at least **WhatsApp.**

You can also send the data as an attachment to a wholly encrypted email (either set up in your usual system by your ICT or through online providers like protonmail.com or tutanota.com).

## HOW TO SECURELY BACKUP/ SHARE DATA ONLINE?

**Data sent to and received from online storage (the "cloud") can be intercepted by hackers, infrastructure's staff and closed-source cloud provider's staff.**

Encrypt your data before storing it on a cloud. User-friendly, free and open source solutions like Cryptomator, CryptSync or cppcryptfs will do it automatically for you in the background.

You can also opt for an open-source cloud solution, secure and respectful of privacy by design, such as owncloud.org, nextcloud.com, Sync.com, AllSync or Cryptomator Enterprise. Some have collaborative tools similar to Microsoft Office 365.

## HOW TO SPOT A PHISHING ATTEMPT?

Dismiss emails from odd addresses, check if links or attachments are legitimate before opening. Ask for advice if you are not sure about a suspicious email.

## HOW TO SECURE YOUR DEVICE'S DATA IN CASE IT IS LOST OR STOLEN?

**Encrypt the whole laptop, a hard drive (internal or external), or a specific zone on your hard drive.**

The best solution as of 2019 is VeraCrypt: it has the best encryption, it is free and easy to use, and audited by leading experts (https://www.veracrypt.fr)

## HOW TO CREATE A SECURE PASSWORD?

**A password/passphrase (i.e. a long password) should be easy to remember but hard to guess by humans/machines.**

**Avoid:** easy patterns (e.g. 1234567), name of the user or their relatives/pets, email address, phone number, birth date, hobby, proverbs, books quotes, song titles and their combinations (these are the keywords that hackers will try first).
Also avoid writing the password on a paper or in a plain file on the computer.

**Include:** lower/upper case letters, digits, punctuation, special characters, typos and unusual words. The longer the passphrase and the more unusual words/characters in it the better.

**Use:** password management tools such as https://keepass.info

## HOW TO DESTROY DATA?

**Use file "shredders" that will actually destroy data bytes. Deleting normally, even when trash is emptied, will only "forget" the file but not destroy it.**

Examples: https://eraser.heidi.ie/download/

## WHICH SOFTWARE IS BEST TO USE?

Always prefer open source software. Its data processing is transparent and can be audited by independent specialists.

## CREATE A DOCUMENT ACCESS POLICY

- Define access rights.
- Document and map your data and its access policy.

## SPLIT YOUR DATA FILES

- Try to keep identifying data, as well as geographic and personal information in separate files.
- Share only what is truly necessary.

## SECURE TABLETS

Use the built-in device encryption in Android and set field encryption in ODK-based survey software.

CAMEALEON Caritas Lebanon SOLIDARITÉS INTERNATIONAL OCHA UNHCR The UN Refugee Agency Inter-Agency Coordination Lebanon