CTIP M&E Toolkit: Checklist for Data Privacy and Security (Jessie Brunner, 'Getting to Good Human Trafficking Data' and USAID 'Monitoring Toolkit, Data Security Guidance: Protecting Beneficiaries')

This document contains a checklist of considerations to take into account when designing a data management plan for a MEL project, especially in issues regarding data security, data storage and data sharing. For further explanation on these, please refer to the 'CTIP M&E Toolkit: Summary of Data Privacy and Security' document.

Data Management Plan

- Do you have a Data Management Plan?

Checklist of potential components of your Data Management Plan:

- ☐ Consent procedures
- ☐ Data inventory
- ☐ Data archiving plan
- ☐ Data disposal plan
- ☐ Data security plan
- ☐ Inventory of hardware and software
- ☐ Established naming convention(s)
- ☐ Defined list of people that access the data.
- ☐ New staff training and awareness plan and records
- ☐ Management plan for organizational data on personal devices, including when staff leave?
- ☐ Internal and external data sharing and disclosure processes
- ☐ Case data management plan
- ☐ Awareness of and adherence to the relevant governing policies or regulations
- ☐ Data quality plan, including data cleaning.
- ☐ Backup plan? Are the same security and privacy measures in place for the backup copy?
- ☐ Appropriate management plan for sensitive information, including storage offline

Data Security

Organization's practices around data security

Organization's practices and protocols

- Do you have an appropriate, robust periodic assessment of your organization's current practices around security?
- Do you revise protocols to mitigate potential new risks at key moments, such as when new features are added to your data systems or when organizational policies or programs change.

- Do you spot any potential vulnerabilities or threats? Do you have a plan for how to address those potential concerns?
- Are your staff coached on data security protocols?
- Do you have guidelines or manuals you use to train new staff?
- Do you ensure all staff and partners have a basic working knowledge of cybersecurity best practices?
- When sharing devices, does each user have unique log-in credentials and passwords or passphrases to track data access?

Legal considerations:

- Have you consulted the national and regional legal frameworks when designing your data protection policies?
- Do you check the laws in the place(s) where you are registered, operate, and store the data and where your clients/subjects reside?
- Do you have a comprehensive understanding of legislation on digital data?

Emergency plan for data breach

- Is there an appropriate plan to deal with data breaches or other security emergencies? Would you know who to consult with to operationalize this plan?
- Is there an appropriate plan to deal the loss of a device containing sensitive information?
- What protective resources can you provide to data subjects whose data has been compromised?

Secure physical environment

- How do you guarantee the security of your offices and work environments?
- Have you restricted access to offices and workspaces? (i.e., via the use of key fobs).
- Are your Wi-Fi network and password information displayed in public places?
- Do your devices lock automatically when inactive?

Individual practices around data security

- Do you require the use of long, unpredictable, and complex passwords (mixing character types such as numbers, letters, and special characters)?
- Do you use an additional layer of log-in security such as through biometrics?
- Do your personal devices secure automatically if they contain sensitive data related to your work?
- Does your computer, smartphone, or other devices lock automatically after a short time interval and use password protection to log in?
- Do you encrypt your data? Have you consulted the legal norms in your area regarding data encryption?
- Have you encrypted all electronic devices accessing sensitive data?
- Do you store in encryption tools the password-protected or encrypted individual documents and folders?
- Do you forbit the sharing of account credentials between users?

- Are you familiar with 'phishing' practices? Do you know how to prevent it? Do you train your staff regarding this?

Deleting/Destroying Data

- Do you ensure deleting or destroying paper and electronic copies of PII once their purpose has been accomplished?
- Do you shred documents following transcription, use, or required storage period?
- Do you destroy your data securely and responsibly?
- Do you use wiping tools to ensure you remove digital footprints? Do you erase secondary devices such as flash drives or digital cameras?
- Have you checked the personal data privacy laws in your area?

Protecting identities of data subjects

- Are policies in place to safeguard potential sensitive or personally identifiable information?
- Do you collect and report only the needed amount of PII data?
- Do you anonymize the data that you collect? Do you use a unique identifier code?
- Is the matching of anonymized data or codes stored separately from the original name's information? Is it encrypted and store securely separately from the full data set?
- Is access to PII strictly limited to only the staff who need it?

Data Storage

Hard copies of information

- How and where do you store your paper files to prevent theft, loss, or damage?
- Are documents stored in filing cabinets in a restricted-access workplace?
- How is access to documents managed and regulated?
- Are all documents routinely collected from public spaces (i.e., following workshops, trainings, etc.) leaving none behind for disposal in contracted facilities (such as hotels)?

Soft copies of information

- Are you aware of the different options to store digital data? Do you know the advantages and disadvantages of each of them?
- Do you use long, unpredictable, and complex passwords (mixing character types such as numbers, letters, and special characters)?
- Have you encrypted all electronic devices accessing sensitive data?
- Do you encrypt email attachments?

Data Sharing

- Have you established protocols to govern why, how, when and with whom are you sharing the data?

- Have you created a data-sharing plan? Is there a person appointed to oversee this in your organization? Have you established a set of norms and standards for this?
- Do you ensure whether your partners have appropriate safeguards in place to secure the data collected?
- How do you guarantee PII data to be protected when being shared?
- Do you get permission from the data subject to disclose their information?
- Do you de-identify the data subjects to protect their identity? How do you do this process?
- Which method do you use to share your data? Do you use encryption for this?
- Do you ensure attachments to emails are password protected?
- If using cloud services do you encrypt the files before uploading them to the server?
- Do you ensure access permissions to only appropriate team members for a determined period of time?