DATA PROTECTION PROTOCOL (ISP ANNEX)

This protocol is intended for programs to assess their existing data security and develop a customized data protection protocol. This is designed to be an active document that complements your other Data Protection Protocols/Policies. At the time of establishing the GBVIMS/Primero, programs should adapt this template for their context.

GENERAL DATA PROTECTION	
	Staff have been asked to identify security risks specific to their context and to explicitly think through the possible implications for clients, their families and communities, and for the organization, if data gets into the wrong hands.
	All staff in contact with the data have a strong understanding of the sensitive nature of the data, the importance of data confidentiality and security.
	Staff understand that all cases will be allocated a code based upon an agreed standard coding format, and that the code should be used to refer to the case either verbally or on paper, in place of any identifiable information such as name.
	Clients and/or their caregivers are giving their informed consent for the agency/agencies to gather and store their data before any information is recorded. Staff are aware that when obtaining informed consent, clients may highlight particular information that they do not want shared with certain people, and that this must be recorded and respected. Signed paper consent forms are being kept in a locked filing cabinet.
	Information is not being passed to a third party without the informed consent of clients and/or their caregivers and following the data sharing protocols of the GBV program.
	All staff working with data sign the data protection checklist/agreement as part of their hiring process.

PAPER FILE SECURITY	
	Paper documentation for each incident is stored in its own individual file, clearly labeled with the incident number. Names of clients are NOT on the outside of the paper files.
	Paper files are being kept in a locked cabinet / drawer, accessible only to responsible individuals specified by the Managers. No one else should be given independent access to the paper files without permission. For the GBVIMS, intake and consent forms must be stored separately.
	Rooms containing paper and electronic information are being locked securely when the staff leave the room. All staff are aware of the importance of being vigilant as to who is entering the room where they work and for what purpose.

ELECTRONIC DATA SECURITY	
	All computers being used for data storage are protected with strong case sensitive and special character-included passwords.
	All applicable staff are aware that information should be transferred by encrypted and password-protected files whether this is by internet or USB/memory sticks.
	At least two backups exist – one stored in the location of the database and backed up each week data is entered, and the second sent for secure storage in a designated off-site location (for example: the database copy sent to GBV Program Coordinator or GBV Information Management Specialist once a month). Staff responsible for the data at the second site must follow the same Data Protection Protocols. The reason for having an off-site back-up is so that the main database can be restored in case of technical problems, or destroyed in an emergency evacuation without this meaning the loss of all electronic data. Typically, the on-site back up is an external hard drive which is kept locked in a filing cabinet, and the off-site back up is done through emailing the database to the designated receiver (most likely GBV Coordinator) as an encrypted, password-protected file.
	All computers have antivirus protection installed and active.
	Ensure all computers have the latest software updates and security patches. You may also confirm that Windows Update is correctly configured to download updates automatically, and then periodically check for errors or failed updates.
	If using tablets in your setting, ensure all devices are encrypted from the lock screen, set up app lock, and enable a device manager in case the device is lost or stolen to enable features to find it or erase data.