JOYFUL HEARTS ORGANIZATION

Data Backup Plan

Version 01

Name of Program: Malindza TB/HIV Project

Date of Original Plan: February 30, 2014

Date updated: April 15, 2014

Table of Contents

Contents

1. Background

It is JOYFUL HEARTS ORGANIZATION policy to protect its information. Therefore the organization is taking responsibility for the development and implementation of backup procedures that are consistent with the overall policies and procedures guiding the organisation. Furthermore, our organization is committed to employ all appropriate backup strategies for anticipating and controlling crisis situations. Our potential data security risks are as follows;

- Virus attack
- Fire
- Theft of computers
- Failure of computer hardware or software
- Deliberate data manipulation
- Power failures
- Lightning attacks

2. Purpose

JOYFUL HEARTS ORGANIZATION places a high importance on secure storage of all collected data and maintenance of confidentiality on information the staff encounters in the course of offering data entry and manipulation of data. All JOYFUL HEARTS ORGANIZATION staff has undergone training on security of patient data confidentiality and security guidelines and refresher courses shall be organized regularly. JOYFUL HEARTS ORGANIZATION aggregate databases are password protected and regular off-site back-up procedures have been put in place to ensure that data will not be lost in case of system failure.

3. Data Backup Types

JOYFUL HEARTS ORGANIZATION will backup all data that is deemed useful no matter how insignificant it may seem. Data from HTC, adherence support, program documents, financial documents, correspondence, study/research data and inventory will be backed up.

Data Type	Frequency of Back - Up	Location of Data	Data Format (pdf, word, Excel, etc.)	Person Responsible
HTC Clients	Once a week		Excel	M&E Officer
Adherence Support Clients	Once a week		Excel	M&E Officer
Program Documents	Once a month		Word & pdf	Program Director
Financial Documents	Once a week		pdf	Finance Admin
Correspondence	Once a month		word	Program Director
Study/Research Data	Once a month		Pdf/software	Program Director
Inventory	Once a month		word	Finance Admin

4. Guidance on Final Documents and Retention

Program files will be saved in both WORD and PDF all the time by the responsible person. Files on excel will have passwords for reliability purposes. The Program Director with the assistance of the M&E Officer will ensure that all final documents are in compliance with the organizational procedure. All documents, including electronic documents will be kept for five years before they can be destroyed.

Data will be filed according to the date the final document was authored and the program. For example; Implementation Plan Final August, 31, 2013

5. Ownership Roles & Responsibilities

The Program Director is the ultimate person responsible for data backup. However, the M&E Officer and the Finance Administrator will be responsible for their respective documents under the supervision of the Project Director.

Data Back –up responsibility or function	Person Responsible	Alternate Person Responsible
Program Documents	Program Director	M&E Officer
Financial Documents	Finance Administrator	Program Director
M&E Documents	M&E Officer	Program Director
Correspondence	Program Director	M&E Officer

6. Data Backup Process

HTC and Adherence Support Data will be entered into a Database that will be accessed by only the Project Director and the M&E Officer. Program Documents and Correspondence Data will be converted to pdf and saved into an external drive. As a matter of standard practice, all data will be stored in an external drive coded according to the function it has.

7. Onsite and Offsite Back-up

Data Back Up Issues	On Site	Off -Site
What data storage medium will be used for back-up?	External Hard Drive	Drop box/Skydrive
Where will the back-up be stored?	Lockable Drawer	Drop box
How often will the back-up be conducted?	Once a week	Drop box
Who is responsible for offsite back-up back up?	Program Director	Drop box
Who is the alternate person responsible for back-up back up?	M&E Officer	Drop box

8. Data Backup Audit Trail and Verification

The implementation of the project activities will be documented in JOYFUL HEARTS ORGANIZATION Program Descriptions COP Narratives, COP Indicators, monthly work plans, MER Plan, Implementation Plan, and an M&E Routine Schedule. Consultation with relevant stakeholders i.e. CANGO/PACT, Malindza Refugee Clinic will continuously update these documents to reflect changing needs and demands. The details of quality assurance and quality improvement activities will be guided by the national quality assurance framework and will be implemented as per specific DQA SOP.

9. Managing back up failure

In the event of hardware or software failure resulting in data loss, JOYFUL HEARTS ORGANIZATION will seek the services of specialist in Data Management. These Data Specialists are:

Matmo Investments (Pty) Ltd.
Trading as Metrofile
Mdlebe Street
Plot: 448
Mbabane

P. O. Box 6484
Mbabane
H100

Telephones
+268 7602 6163
+268 2404 6114
+268 7605 2290

Fax: +268 2404 1077
Email: acsd@swazi.net

10. Data Security

All computers have ANTIVIRUS protection. The software being used is the Norton by Symantec valid for 1 year. BUSCITECH is responsible for installing and updating anti-virus software. There is an amount set aside for anti-virus software as part of the soft ware and web pages development in the budget. The computers automatically update the virus once a week as the anti-virus was created that way, however, there is a routine manual updates made every Friday checked by the M&E Officer.
The Program Director and M&E Officers use their personal passwords to protect data. Data on excel is password protected using email addresses and the passwords of the authorized personnel.

11. Operationalising the Data Back –up Procedure

Staff members will be informed about the Data Back-up Procedure during review meetings. The M&E Officer will be responsible for sharing with team members. The procedure will be reviewed once every three months during review meetings.

12. What are the "Don'ts" for the Back-up procedure?

- Use of back-up storage devices for personal use or transfer documents from one computer to the other
- Forgetting to randomly check whether back-ups are being done?
- Backing up different files in one folder.
- Forgetting to change word documents to pdf before being backed up.
- Keep the back-up storage with anyone anytime.