# DATA SECURITY & PROTECTION POLICY MERCY HANDS FOR HUMANITARIN AID

## Introduction

Data Security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites, such as encryption, key management, locked doors, tamper-proof, firewalls, passwords, logical, physical, privacy screen filters or secure erase and asset disposal; while Data Protection is the process of safeguarding important information from corruption and/or loss, such as backup, snapshots and replication.

Mercy Hands data protection & security guidelines seeks to protect the interests of Mercy Hands and its beneficiaries. To enhance Mercy Hands operations and systems, data security and protection should be applied systematically throughout the organization.

## Definitions

- Confidential Data: any financial or accounting documents, or documents that contain personal identifiers of Mercy Hands' staff, partners, contractors, donors, or beneficiaries. Both soft and hard copy documents are included in this definition.
- Personal Identifiers: names, addresses, phone number, e-mail addresses, pictures, and alike.

## Mercy Hands' Commitment

Mercy Hands shall take all reasonable and necessary precautions to preserve its work and confidentiality of personal data of its staff and beneficiaries. All personal data shall be collected, used, transferred and stored securely in accordance with the Mercy Hands data security and protection principles.

## Responsibility

Data security and protection is the responsibility all Mercy Hands' personnel, staff, Board members, and volunteers. Enforcing Mercy Hands Data Security and Protection Policy is the responsibility of IT Unit. The IT Unit is one of the administrative departments. The IT Officer works under the overall supervision of the Executive Administration and s/he reports directly to the General Administrator.

## Mercy Hands' Data Security and Protection Principles

1 LAWFUL AND FAIR COLLECTION

Personal data must be obtained by lawful and fair means with the knowledge or consent of the data subject.

2 SPECIFIED AND LEGITIMATE PURPOSE

The purpose(s) for which personal data are collected and processed should be specified and legitimate, and should be known to the data subject at the time of collection. Personal data should only be used for the specified purpose(s), unless the data subject consents to further use or if such use is compatible with the original specified purpose(s).

3 DATA QUALITY

Personal data sought and obtained should be adequate, relevant and not excessive in relation to the specified purpose(s) of data collection and data processing. Data controllers should take all reasonable steps to ensure that personal data are accurate and up to date.

4 CONSENT

Consent must be obtained at the time of collection or as soon as it is reasonably practical thereafter, and the condition and legal capacity of certain vulnerable groups and individuals should always be taken into account. If exceptional circumstances hinder the achievement of consent, the data controller should, at a minimum, ensure that the data subject has sufficient knowledge to understand and appreciate the specified purpose(s) for which personal data are collected and processed.

5 TRANSFER TO THIRD PARTIES

Personal data should only be transferred to third parties with the explicit consent of the data subject, for a specified purpose, and under the guarantee of adequate safeguards to protect the confidentiality of personal data and to ensure that the rights and interests of the data subject are respected. These three conditions of transfer should be guaranteed in writing.

6 CONFIDENTIALITY

Confidentiality of personal data must be respected and applied at all stages of data collection and data processing, and should be guaranteed in writing. All Mercy Hands staff and individuals representing third parties, who are authorized to access and process personal data, are bound by confidentiality.

## 7 ACCESS AND TRANSPARENCY

Data subjects should be given an opportunity to verify their personal data, and should be provided with access insofar as it does not frustrate the specified purpose(s) for which personal data are collected and processed. Data controllers should ensure a general policy of openness towards the data subject about developments, practices and policies with respect to personal data.

## 8 DATA SECURITY

Personal data must be kept secure, both technically and organizationally, and should be protected by reasonable and appropriate measures against unauthorized modification, tampering, unlawful destruction, accidental loss, improper disclosure or undue transfer. The safeguard measures outlined in relevant Mercy Hands policies and guidelines shall apply to the collection and processing of personal data.

## 9 RETENTION OF PERSONAL DATA

Personal data should be kept for as long as is necessary, and should be destroyed or rendered anonymous as soon as the specified purpose(s) of data collection and data processing have been fulfilled. It may however, be retained for an additional specified period, if required, for the benefit of the data subject.

## 10 APPLICATION OF THE PRINCIPLES

These principles shall apply to both electronic and paper records of personal data, and may be supplemented by additional measures of protection, depending, inter alia, on the sensitivity of personal data. These principles shall not apply to non-personal data.

## 11 OWNERSHIP OF PERSONAL DATA

Mercy Hands shall assume ownership of personal data collected directly from data subjects or collected on behalf of Mercy Hands, unless otherwise agreed, in writing, with a third party.

## 12 OVERSIGHT, COMPLIANCE AND INTERNAL REMEDIES

An independent body should be appointed to oversee the implementation of these principles and to investigate any complaints, and designated data protection focal points should assist with monitoring and training. Measures will be taken to remedy unlawful data collection and data processing, as well as breach of the rights and interests of the data subject.

## 13 EXCEPTIONS

Any intent to derogate from these principles should first be referred to the Country Director for approval, as well as the Executive Director of Mercy Hands.

## General Staff Guidelines

Employees should keep all data secure, by taking sensible precautions and following the guidelines below:

- The only people able to access data covered by this policy should be those who need it for their work. The General Administrator is authorized by the Executive Director to give authorization to staff accessing protected data.
- Confidential data must be stored in a secured cabinet and placed in a room that can be locked.
- All rooms that contain confidential data must be locked after working hours. One or more of the occupants of the room will be assigned a key to the room and they will be responsible for locking the room at the end of the work and making sure that the room is never left unattended at any time. The key assignees will be held accountable for any loss of confidential data that is not due to forceful break-in.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- All electronics (laptops, desktops, cameras, data storing devices, etc.) that contain confidential data should be protected by strong passwords and the staff responsible for the electronics must not share these passwords with anyone. If the password is compromised or the electronics is stolen or lost then the responsible staff must report the incident to the IT Officer and update their passwords immediately.
- Personal data should not be disclosed to unauthorized people, either within Mercy Hands or externally.
- Employees should request help from their line manager or the IT officer if they are unsure about any aspect of data protection.
- Any suspected compromise of data security has to be immediately reported to the IT Unit or the Executive Administration.
- The Security Department shall work with the IT Unit to reinforce data security by applying any physical

## Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT Officer.

When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Computers should be protected by strong passwords that are changed every six months and never shared between employees. The IT Officer will send e-mail to all employees every six months reminding them to change the password.
- If data is stored on removable media (like a USB or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with Mercy Hands' standard backup procedures.
- All servers and computers containing data should be protected by approved security software and a firewall.

## Data Archiving and Backup

Data archiving is the practice of moving data that is no longer being used to a separate storage device, while Data Backup is the practice of copying files and folders that are still in use for the purpose of being able to restore them in case of data loss.

The following is general guidelines of data archiving:

- Data archiving and backing up is the responsibility of the IT Unit.
- The General Administrator defines what documents that need to be archived or backed up.
- The IT Unit is responsible for setting up and regularly maintaining a system for data archiving and another system for data backup.
- Access to archived data is restricted to Board members, Executive Administration, and those authorized by the General Administrator.