Technology Policy

Purpose

Mercy Hands seeks to effectively manage the computer system for guiding the use, maintenance and security of the computer equipment. The IT Manager is responsible for ensuring that the procedures and policies suggested here are followed.

Use

Using computer equipment requires particular care because of its fragility and high cost. Access to the equipment should thus be strictly reserved to Mercy Hands employees only. Those employees who are unable to handle commonly-used software will be given an orientation by the IT staff on request.

Security

A. In order to safeguard the computers against viruses, only external drives belonging to Mercy Hands are to be used.
B. In order to safeguard computers from viruses, antivirus software should be installed in the computers. It is the duty of the employee to ensure that it is updated regularly.
C. All documents should be kept on Google Drive with ownership transferred to Mercy Hands.
D. Mercy Hands emails should not be used to create personal accounts and should only be used on trusted websites. If unsure, please contact the IT Department.
E. The IT Manager must approve all accounts being made with Mercy Hands email.
    a. Accounts that are to be used by the entire organization should be made with info@mercyhands.org email.
F. Usernames and passwords should be emailed the IT Manager to ensure that they are tracked and accessible at all times.
G. Should an employee believe that they have been subject to a hacking or phishing attempt, they must contact the IT Manager Immediately.
H. Before clicking on email links, the employee should verify that it comes from a trusted email.
I. Passwords should be updated every 6 months to ensure privacy.

Two-Factor Authentication

Whenever possible, employees should enable two-factor authentication on all work related accounts to ensure privacy and security.

Handling Secure Information

When handling personal data, extra steps will be taken to ensure the security of the documents and data. Information may be deemed secure by the Executive Director, donor, or partner organization. If there is doubt about the sensitivity of information, it should be treated as secure. This policy will be in line with the donor and/or partner data protection and safety regulations. Should one of those be found to be stricter, it should supersede this document.

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

1. Secure information may not be sent or downloaded on public wifi.
2. Secure information may only be accessed on accounts with two-factor authentication enabled.
3. Secure information must be stored on encrypted computers and sent via encrypted software.
4. People whose information is being stored will be informed of all protection measures, and their limitations, and will have the ability to willingly consent to give, or not to give, their data. The consent will be written when possible and may be withdrawn at any time without reason.
    a. For personal information stored on minors, the minor must be above 16 years of age to consent to their information being stored. For people 15 years or younger, parental consent must additionally be obtained.
5. Personal data will be erased when it is no longer necessary to be stored and only necessary data will be collected.
6. Personal data will only be used for the purposes that the person has consented to. Use for any other purpose will require consent from the person.
7. When possible, the data will be pseudonymized.
8. People will have access to the information stored on them upon request.
9. A record of the data processed shall be maintained.

10. The IT Manager will take all necessary steps to regularly evaluate Mercy Hands' ability to keep data secure, if its ability is found to be insufficient, all collection and processing of personal data will be immediately halted until remedial measures are taken.
11. Only employees deemed necessary will have access to personal data. This data will not be made publicly available.
12. Should Mercy Hands be made aware of a breach, people whose data has been impacted as well as a supervisory authority will be immediately notified.
13. When sharing data with external organizations, Mercy Hands will first ensure that they have the necessary ability to secure the information.
    a. Should Mercy Hands find that they are not securely storing the information, they will immediately cease information sharing with them and discontinue future information sharing.
14. Employment data is also considered personal data and will be protected as such. Information on data protection will be given to employees when signing employment contracts.

Khaldoon Al-Moosawi
Executive Director

Reviewed: June 2022