Training of Health Researchers into Vocational Excellence in East Africa (THRiVE) Information Technology Policy

THRIVE

TRAINING HEALTH RESEARCHERS INTO VOCATIONAL EXCELLENCE IN EAST AFRICA

March 2014

Supported by
wellcome trust

Contents

1. Introduction 3
2. Who does this policy apply to? 3
3. What does the Policy Cover? 3
4. User Responsibility 4
5. 5. Licensing and copyright 5
6. Access to Data 5
7. Data Storage 6
8. Removal of data 7
9. Data Loss 7
10. Procedures for managing data security breach 7

1. Introduction

Training Health Researchers into Vocational Excellence in East Africa (THRiVE) is a Wellcome Trust (WT) funded Institutional Capacity building consortium, with Makerere University as lead partner. Other partner institutions include: Kilimanjaro Christian Medical College, National Institute of Medical Research at Mwanza, International Center of Insect Physiology and Ecology (icipe) Nairobi Kenya, National University of Rwanda, Gulu University, Uganda Virus Research Institute, Cambridge University and London School of Hygiene and Tropical Medicine.

In an effort to ensure security of all technology and information procured and/or supported by THRiVE funds, THRiVE secretariat at Makerere University has put together an Information and Technology Policy to guide the use of technology and acquisition, access, process, and storage of information. The policy was developed in consultation with Makerere University Directorate of Information and Communication Technology (DICTS), with technical support by the Wellcome Trust IT Service Delivery & Operations manager. The policy lays out the responsibilities of persons who use technology or handle information that are acquired partially or fully using THRiVE funds. Each person has a responsibility for making informed decisions and ensuring that THRiVE Technology and any information acquired or accessed, is handled securely and responsibly, especially when data and information is of a sensitive or confidential nature.

1. Who does this policy apply to?

The policy applies to staff, fellows, individuals conducting THRiVE supported work, and any other person who use technology or personal devices to acquire, access, process use or store data and information in any format provided it is supported or aimed at achieving THRiVE objectives.

2. What does the Policy Cover?

ICT Resources referred to in this policy include but are not limited to:

a) Computers and mobile devices (Laptops, iPads, PDAs, mobile phones)

b) Software
c) Databases
d) The Network and related network services
e) USB Storage Devices

This policy also covers the data and information accessed or held within these devices, or information hosted by authorized third parties (Cloud). It also includes paper or hard-copy information held on or off-site.

Please note that this policy may not cover all situations or answer every question you may have about using technology devices or Trust data. Therefore, if you have a situation that is not addressed by this document or you simply have a question about data security, please call the IT Service Desk or the Information Governance Manager.

3. User Responsibility

Users are responsible for the security and safe keeping of any technology acquired with THRiVE funds used for acquisitioning and/or accessing and storing data and information. To ensure physical security of technology the following measures should be used:

1. Installation of surveillance cameras
2. Secure locking of computers on work stations
3. Permanent Asset Tagging of computers and other accessories

Users must ensure that equipment used to collect, store, access and manage consortium data and information adhere to the minimum data security standards that include:

a) Password Protection: Your computer other mobile devices (IPADs, PDAs, Mobile phones) should be password protected to avoid unauthorized users from gaining access to confidential information
b) Anti-virus: A user PC or laptop MUST have a licensed operational and updated anti-virus and regular virus scan performed

c) Data safety: Your data MUST be encrypted and regularly backed up on either a secondary drive kept separately, preferably under lock and key or on an icloud backup system (dropbox, knowhow, etc)

d) Avoid using untrusted USB drives in your computer

e) Ensure that you ONLY use the industrial recommended power adapter for your laptop and other computing devices

In the event where personal technology devices are used to collect, store, access and manage consortium data, you are responsible for keeping all data and information accessed or stored on those devices secure and in accordance with the requirements of storage of data as outlined below.

4. 5. Licensing and copyright

THRiVE follows a strict policy on the purchase and installation of computer software to ensure that it meets the legal and contractual obligations. When installing or using software on THRiVE technology equipment, you must ensure that the software is properly licensed.

5. Access to Data

Depending on your role you may be given permission to access THRiVE network level data including: financial data, students' records, research and project data, etc. In case were passwords are used to access such data they must not be disclosed or shared with any other person.

Authorization to access, modifications, disclosure and destruction of data will depend on its sensitivity. To ensure confidentiality and integrity, different levels of access to data are defined.

Level 1: Data with low sensitivity

Access to this data is granted to any applicant and can be published with minimal or no restrictions. This can be considered as public data. Concerns should be more on integrity therefore the responsible party in charge should authorize replication or copying to maintain accuracy.

Level 2: Moderate sensitivity

Access to this data must be requested for and authorized by the relevant party or unit responsible. Nonpublic or internal data is considered moderately sensitive. Access can be granted basing on job classification or responsibility (role based access). Data/ information that can be considered as level 2 may include but not limited to;

- Research data and other project information,
- Official institutional records such as financial reports, budget information, human resources information.

Level 3: Data with high sensitivity

Access to this data is controlled during the creation all the way to its destruction and is accessed by only those affiliated with the institution and require access to it to perform their job. This information may be restricted by state law. Data/ information that can be considered as level 3 may include but not limited to;

- Student records
- Student grades data
- Individuals' Health information
- Human subject research data
  - In situations where human subjects are involved as Research Participants the country level and institutional review committee guidelines for research involving human subjects will provide a framework to facilitate the carrying of such research without compromising the rights and welfare of individuals participating or whose data are being used in research.

6. Data Storage

Any sensitive or confidential data or information which could cause financial or reputational damage if lost, stolen or misappropriated must only be stored on the appropriate institutional network or authorized technology devices. Storage on personal devices, such as laptops, external hard drives, unencrypted USB flash drives, mobile phones, CDs or DVDs are not appropriate storage solutions for sensitive or confidential data and may only be used for non-confidential data and information on an occasional and short-term basis.

7. Removal of data

All users of THRiVE information are required to ensure that security measures for the transfer and storage of information are appropriate to the risks faced in that process. If you are uncertain about these risks you must seek advice from your manager.

In addition, all staff have a responsibility to consider security implications when disposing of information in the course of their work.

If you should leave the THRiVE consortium, you will be required to sign a personal undertaking, stating that all THRiVE data and information has been returned and where applicable deleted from all personal devices used.

8. Data Loss

Although THRiVE takes all reasonable steps to prevent data from being misappropriated, you should treat all THRiVE equipment as your own.

Users are responsible for the security and integrity of all technology or personal devices used to access any of THRiVE information systems and applications and the integrity, quality and security of the data and information contained within them.

In addition, all confidential and sensitive hardcopy paper records and information must be protected from unauthorized access and stored securely at all times.

If you believe any of your THRiVE technology, personal devices/hard-copy or paper records has been lost or stolen, you are required to follow the procedure as stated in the procedures for managing data security breach.

9. Procedures for managing data security breach

In case of a security breach, guidelines and procedure to follow include:

a) Immediate notification of the breach to the director of THRiVE

b) Containment and recovery from the breach by the THRiVE IT officer

c) Assessment of the ongoing risk by the THRiVE IT officer