



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

THRiVE Minimum benchmark standard for computer and information Security



March 2014

Supported by
wellcometrust

THRiVE Minimum benchmark standard for computer and information Security

All computing devices fully or partially procured by THRiVE funds or any computers used to perform THRiVE activities must comply to the following minimum security requirements to ensure safety of the equipment and data.

1. **Software installation**
Computers and other computing devices that support software installation must only run licensed software whether proprietary or open source. Pirated and other software should not be used on these devices
2. **Anti-malware/ Anti- virus Software**
Devices installed with an operating system (windows OS, Mac OS, etc) which an anti-malware/ anti-virus software is available, a licensed anti – malware/ virus software must be installed
3. **Update of anti-malware/anti-virus and regular scan of devices**
The anti-malware software must be regularly updated/renewed and regular device scans must be performed
4. **User Authentication**
User access to devices or systems on the devices must require authentication through an authentication mechanism such as passwords and passwords must not be shared amongst users.
5. **Unattended console sessions**
Devices must be configured to lock or logout and require authentication to access if left unattended to for more than 5 minutes.
Devices that don't support auto lock or authentication to access such as printers and other appliances may meet these standards through restricted physical access.
6. **User accounts**
Privileged and super user accounts (Administrator, root) must not be used for non-administrative activities. Users must create user and guest accounts under which to perform daily functions
7. **Data backup:**
Regular back up of data (at least once a week) on a secondary drive (network or external drive) and in case of an external drive, it should be kept separately and preferably under lock and key
8. **icloud backup**

Users should create an icloud account (dropbox preferably) to store documents especially all data related to PhD studies

9. Computer locks

It is highly recommended that when using laptops at the workstation or in the field, they should be secured using cable locks (Kensington laptop lock). The lock can be attached to an immovable object or furniture of large size