Document Control

Document Name:	TIER User Account Management Guidance
Compiled By:	Health Systems Governance and HRH Branch
For queries please contact:	Dr R Govender, Riona.Govender@health.gov.za
Date Compiled:	February 2018

Version Control

Date Updated	Version	Updated by	Comment on changes
02/2018	1	National Implementation Team (NIT)	Document Created
04/2019	2	NIT	Name changed to: TIER.Net User Account Management Guidance Removal of reference to 3 tiered system Expansion of explanation of user roles Updating of references to THIS support portal and new Integrated TB/HIV Data Management SOP

Document Approval

Date Approved	Version	Approved by (Name, Signature)	
28/02/2018	V1	Gail Andrews	GAndrews
01/04/2019	V2	Gail Andrews	GAndrews

TIER.NET USER ACCOUNT MANAGEMENT GUIDANCE

Guiding Principles

The purpose of this document is to define the key processes that govern management of user accounts in TIER.Net, a non-networked electronic programme that contain TB/HIV patient information. In addition, this document provides guidance regarding the roles and responsibilities relating to the user access hierarchy for TIER.Net. All prescriptions regarding the management of user accounts in TIER.Net have been consolidated in this document.

Guiding Principles

- The Implementer role should only be a NDOH or NDCS TIER Key Implementer (TKI), or other staff assigned to oversee the THIS process.
- The implementer role cannot be a District Support Partner or other non-governmental employee.
- If the facility does not have a functional printer, all user access forms must be electronically signed and saved. These must then be sent to the (sub)District for printing.
- If Implementers are locked out of the database due to multiple failed password entry attempts, the NIT is to be contacted on: NIT_Support@health.gov.za or via the www.tbhivinfosys.org.za portal.
- The access control in assigning roles follows AGSA requirements.

Existing guidelines

Key THIS guiding documents:

Current guidance documents that support the use of TIER.Net and formally express prescriptions for the TB/HIV information system more broadly, include, but are not limited to:

1. **Integrated TB/HIV Data Management Standard Operating Procedure (Part I & II)**– This document delineated roles and responsibilities re key TB/HIV information system processes, including how to maintain TIER.Net, routine reporting processes, tools for supporting patient management, and the protection of patient confidentiality. Part I refers to processes at a Facility level and Part II at the (sub)District and higher.

2. **TIER.Net User Guide** – This document, which is embedded in the TIER.Net, provides the user with guidance on software functionality.

THIS Support Portal:

The THIS Support Portal (www.tbhivinfosys.org.za) is an online resource for those who regularly manage, utilise, and interact with the TB/HIV information system. The portal has three primary functions:

1. FAQ - This section includes answers to frequently asked questions organized into thematic categories for ease of browsing.
2. Resources and Tools – This section is where critical files, including guidance materials, training slide decks, TIER.Net installers, and other resources, can be found. Some files are available openly, i.e. a user does not need a login to access the documents, and some are available only to users with login details.
3. Contact Us – This section is a place where users can log/submit third-line support queries for the attention of the National Implementation Team (NIT).

Types of user accounts

TIER.Net has three (3) types of user accounts, all of which offer differing functionality depending on the profile of the user. These include:

Implementer – This role is equivalent to a super user. The implementer role has been created only for those who steer the implementation of THIS processes at facility, sub-district, district, or provincial level**.**

1. Who should be an implementer?
    a. The TIER Key Implementer (TKI)
        i. The person with overall responsibility for the TB/HIV information system
    b. The person responsible for installing, upgrading and supporting TIER.Net (other than the TKI)
2. What can an implementer do regarding TIER.Net?
    a. Add, activate, deactivate all level of users (Implementer, Administrator, User)
    b. Modify user details (user names, passwords, facility access)
    c. Create exports with patient identifiers included.
    d. Perform all the activities of the user and administrator.
    e. Restore back up files.
    f. Merge patients.
    g. Move facility Data.
    h. Export name field data in the Excel Export.
3. What are the implementer responsibilities?

    a. Maintain list of users at facility level.
    b. Ensure correct user level access provided.
    c. Keep track/oversight of user access report.

Administrator – This is the middle-level access role. The administrator role is principally assigned to the Operational or Facility Manager, or anyone in a management role other than the Implementer.

1. Who should be an administrator?
    a. The OPM/FM.
    b. (sub)district IM.
2. What can an administrator do regarding TIER.Net?
    a. Add, activate, deactivate level of users (administrator and user).
    b. Perform limited access on system settings.
    c. Modify user details (user names, passwords, facility access).
    d. Merge patients.
3. What are the administrator responsibilities re TIER.Net?
    a. Monitor and keep track of user access via the User Access Report and the Implementer/Administrator Log Report.

User – The purpose of this user account level is to enable routine data capturing and reporting, whilst limiting the number of system settings that can be changed.

1. Who is a user?
    a. Facility Administrative Clerk (AC) responsible for entering data into TIER.Net.
2. What can a user do?
    a. Add patient information to TIER.Net.
    b. Generate line lists and reports.
    c. Modify own user details and passwords.
    d. Create dispatches and back up files.
3. What are the user responsibilities?
    a. Ensure accurate capturing of patient information into TIER.Net from the clinical stationery.
    b. Action line list and reports (refer to the Integrated TB/HIV Data Management Standard Operating Procedure).
    c. Generate and action the data validation reports timeously.

Creating new user accounts

1. Only implementers and administrators are able to create users in TIER.Net.
2. When a new user account is required, the user must complete a 'User Account Control Form' (Annex A).

3. This form must be signed by the Operational/Facility Manager, or relevant Supervisor.
4. Once signed, the form must be kept in the THIS reference file.
    a. The user is given access to the relevant facility that they perform the capturing of data for. In some instances, the user may require access to multiple facilities (i.e. facility x & y and mobile clinic).

Amending user accounts

5. Administrators can make changes to other administrator and user accounts, however administrators cannot make changes to implementer accounts.
6. Only implementers and administrators can modify other users' account information, including:
    a. Modifying passwords
    b. Modifying the security questions
    c. Modifying the user names
    d. Modifying the facility accesses
7. A user can modify their own account information, including:
    a. Modifying passwords
    b. Modifying the security question
    c. Modifying user name

Terminating accounts

The implementer or administrator level users have the option to either (1) delete, (2) deactivate, or (3) lock accounts on the instance of TIER.Net they are accessing.

1. Deleting the account removes the account completely from the computer, but can compromise data integrity as user accounts are linked with data entry and reporting.
2. Deactivating an account is ideal for users having left their role who will no longer be capturing into or using TIER.Net. When deactivating a user, TIER.Net stores their information on the specific TIER.Net database, but that user no longer displays on the main login screen.
3. Locking an account prevents a user from logging in, regardless of whether they enter the correct login and password information.
4. The FM is to review the User Access Report quarterly, and ensure that any active user accounts that have not been used in three months are deactivated.
    a. This policy does not apply to staff on maternity leave, or staff who have been approved to take leave for more than three months with the intention of returning to work.

Monitoring account activity

There are two reports which monitor user access in TIER.Net. the two reports are to be generated each month, according to the Integrated TB/HIV Data Management SOP. All reports are to be kept in the THIS lever arch file.

If the facility does not have a functional printer, all user access forms must be electronically signed and saved and then sent to the (sub)District for printing, and then returned to the facility for filing.

User Access Report:

This report provides a breakdown of when each user has accessed TIER.Net, including the login date, activation status, and both login and log-off time.

1. All users (user, administrator and implementer) have access to this report.
2. This report determines which users have been active or inactive for a given period of time.
3. Generate monthly as required.
4. As part of the review process, the FM/OM must review the active accounts to ensure alignment with the person’s job responsibilities.
    a. If a user is misaligned, the user must be re-assigned to a role that reflects their assigned responsibilities.
    b. The FM/OM must ensure that these adjustments are reflected in TIER.Net.

Implementer/Administrator Log Report:

This report includes a list of time-stamped transactions (that is, actions performed and the user responsible for each action), including when a user account has been amended in any way by an Implementer or Administrator.

1. Generate monthly, and provide interventions were required.

Password management

Each user in TIER.Net, regardless of level, must create a password when creating an account, supported by a ‘forgot password’ question.

1. When a user is setting up their account, they will be prompted to create a password.
    a. The user can change their password when necessary.
    b. Passwords must meet the following criteria:
        - Length of at least 8 characters
        - At least one non-standard character (-\ / @ not allowed)
        - At least one numeric character
        - At least one Uppercase and at least one lowercase letter
2. This password is required each time a user logs into TIER.Net.

3. If a user enters the incorrect password more than (3) times, they will be locked out of the login process.

In addition to the creation of a password, each user is required to create a security question that will be used as a prompt, should the password be forgotten. It is very important the user enters a 'forgot password'' question that they will remember. (e.g. Name of first partner, first pet name, grandmother family name, etc.)

1. A user will have (4) attempts to answer using the 'forgot password' method.
2. In the event both the password, and the 'forgot password' attempts have been reached, the user will be locked out of the system and an Administrator or Implementer need to be contacted in order to unlock the database.

In the event that the implementer, administrator and user passwords and 'forgot password' attempts have been reached, the database will be locked, and will need to be sent to the NIT for unlocking.

1. PLEASE NOTE: This will mean that all capturing for the facility will need to stop until such time that the 'unlocked' database is returned.

Annexure A
TIER.Net User Account Control Form

New users that require access to TIER.Net must complete this registration form. Please complete the form, and ensure that it is signed off by the Facility Manager, or in cases where user access is required above the facility-level, your Supervisor.

TIER.Net User Account Information:

Please fill in the fields below

First name (in full)	
Last name (in full)	
Email address	
Position	
Employer	
PERSAL/Employee Number	
ID number	
Cell phone number	
Preferred username	

Current Action:

Please mark the desired action below with a check mark (see User Account Management Guidelines for definition of actions)

	Activate account
	Delete account
	Deactivate account
	Lock account

User Account Role:

Please mark the appropriate user role(s) below using the fields on the left with a check mark (see User Account Management Guidelines for user definitions)

	Implementer
	Administrator
	User

Acceptance of Terms:

I, ______________________________ (print full name), hereby agree to honour the confidentiality of data housed within TIER.Net, and will not disclose my authentication credentials (password) or data to anyone not authorized to access TIER.Net at a given workstation.

Signature	***Date (DD/MM/YYYY)***

Authorization for User Account Access (to be completed by Facility Manager/Supervisor):

Full Name (first and surname)	***Position/Title***	***Signature***	***Date (DD/MM/YYYY)***