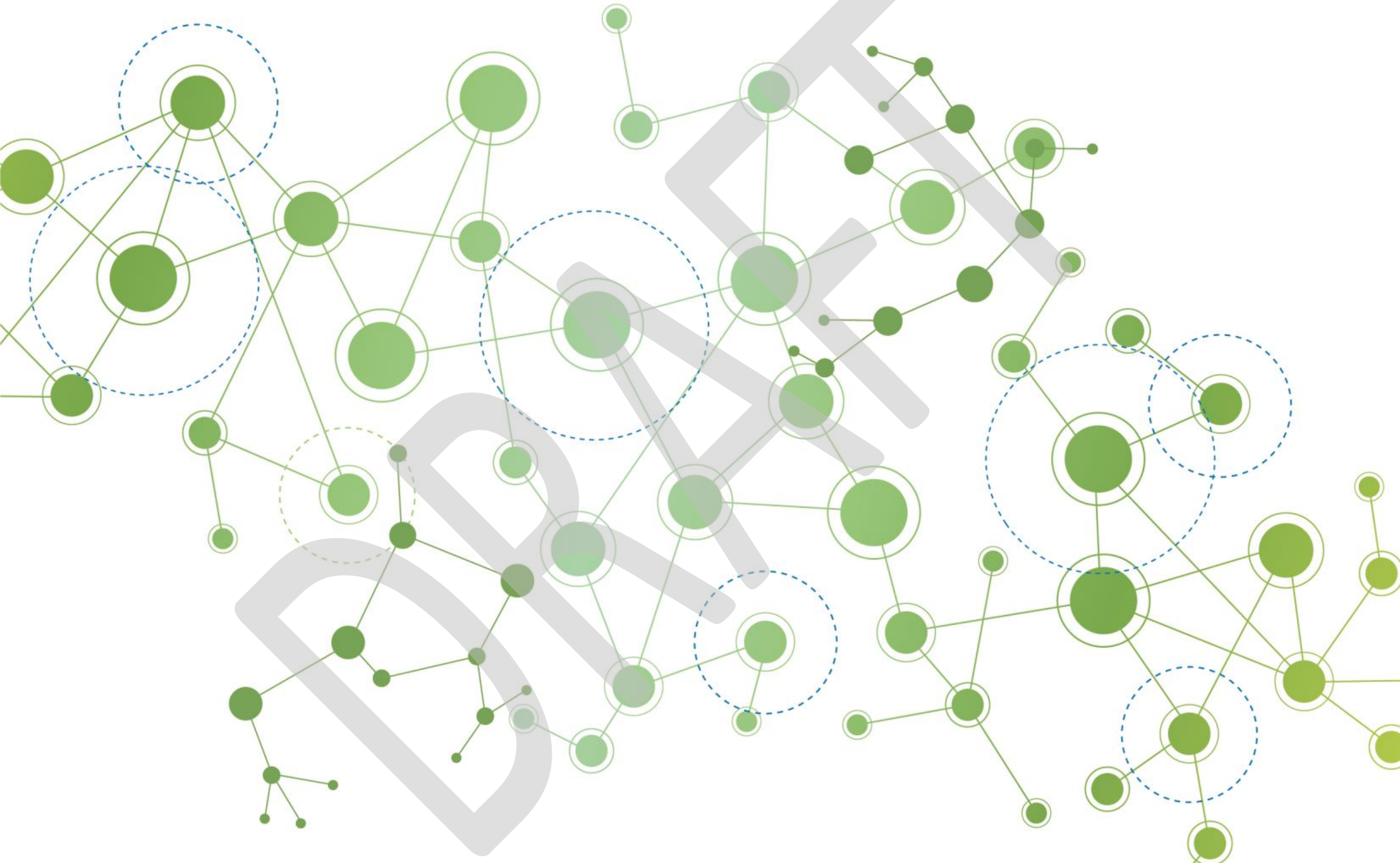
TIER.NET USER ACCOUNT MANAGEMENT GUIDANCE



Enquiries: please contact

Riona Govender ***Riona.Govender@health.gov.za***

health
Department:
Health
REPUBLIC OF SOUTH AFRICA

Document control

Document name:	TIER User Account Management Guidance
Compiled by:	Health Systems Governance and HRH Branch
Contact details for queries:	Riona.Govender@health.gov.za
Date of this version:	01 June 2020

Version control

Date updated	Version	Updated by	Comment on changes
02/2018	1.0	National Implementation Team	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
06/2020	3	Health Informatics Directorate	▪ Revision to AGSA required password control ▪ Refinement to user accounts

Approval

Date approved	Version	Approved by	
28/02/2018	1.0	Dr, Gail Andrews	
01/04/2019	2.0	Dr. Gail Andrews	
15/06/2020	3.0	Dr. Gail Andrews	

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.

- 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.

1. Who should be an implementer?
    a. The DOH staff member responsible with the overall responsibility for the TB/HIV system. This is the DOH allocated staff member responsible for maintaining TIER.Net, including capacitation and training, previously known as a TKI (TIER key implementer).
    b. The person responsible for coordinating the installing, upgrading and support of TIER.Net
    c. This role cannot be assigned to a third party or non-DOH staff member
2. What can an Implementer account user do regarding TIER.Net?
    a. Add, activate, deactivate all level of users (Implementer, Administrator, User)
    b. Modify user details (usernames, passwords, facility access)
        i. This is tracked in the Implementer/Administrator Log Report

    c. Perform all the activities of the user and administrator
    d. Restore back up files if on the same computer.
    e. Merge patients that have been verified and documented.

3. What are the implementer responsibilities?
    a. Maintain list of users at facility level.
    b. Ensure correct user level access provided.
    c. Monitor the user access report.
    d. Coordinate the upgrading of the software and any IT related queries where needed.

Administrator – This is the middle-level access role. The administrator role is principally assigned to the Operational or Facility Manager, or any DOH staff member 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 (usernames, 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 can create users in TIER.Net.

    a. User accounts can be created with a generic username and password.

    b. The User does not need to be present when the user account is being created. However, on first log in, the User will be required to reset their password.

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 usernames

    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 username

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 as per the Integrated TB/HIV Data Management SOP (part I)
   a. This policy does not apply to staff on maternity leave, or staff who have been approved to take leave of absence.

Monitoring account activity

There are two reports which monitor user access in TIER.Net, the User Access Report and the Implementer/Administrator Log Report. The two reports are to be generated as indicated in the Integrated TB/HIV Data Management SOP. All reports are to be kept in the facility based THIS lever arch file.

If the facility does not have a functional printer, all user access forms must be electronically signed and saved. Optimally, the forms should be 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. 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 and provide interventions were required.

Password control policy

1. Password constraints: A password cannot contain the user's full name or username
2. Password history: Prevent the reuse of the user last 12 passwords
3. Maximum password age: Passwords must expire after a defined period to encourage regular password updates. Expiry is age based on the user's role: Users: 90 days, Administrator: 90 days, Implementor: 180 days.
4. Password expiry notification. A user must be notified that their password is due to expire:
5. The user will receive an initial expiry notification seven days before expiry
6. After the initial notification a user will receive a reminder daily for the last three days
7. The user can decide to reset their password or close the notification
8. Expired password. Once a user's password has exceeded the maximum password age, the user will be:
9. Notified that their password has expired and prompt to reset their password
10. Directed to the user to user details screen to update their password
11. If a user decided to not update their password, they would not be able to log in to the system
12. Initial login: When a user logs in with a newly created account, force the user to reset their password.
13. Display a notification to update password and navigate the user to the user details screen.
14. If the user does not update their password and cancels the step redirect to the login screen.

15. The system will validate the entered password preventing the reuse of the initial password provided by the admin/implementer.

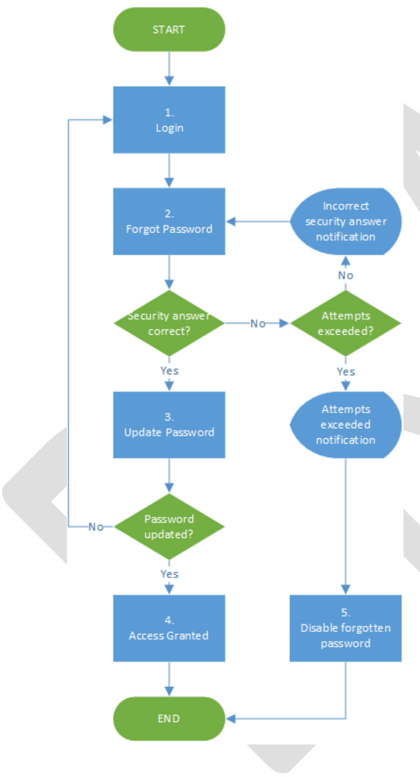
16. Failed password authentication: Incorrect password notification to indicate the number of attempts left be before lockout.

17. Forgotten password:

18. After a correct security question provided, display a notification to update the password. Redirect to the user details screen to complete the password update. Users that complete the process will gain access, if the step is cancelled redirected to the login screen.

Password flow diagrams

FIGURE 1. FORGOTTEN PASSWORD



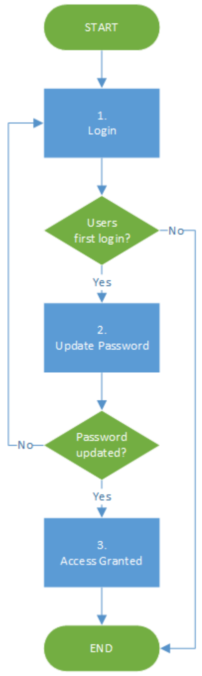
Process Steps:

- User opens TIER.NET, the login screen is displayed, and the user clicks forgot password
- The system displays the forgot password security question:
  - Correct answer provided, display notification to update password and proceed to step 3
  - Incorrect answer provided, display incorrect answer notification with the number of attempts left before the forgot password function is disabled
  - If the user exceeds the security question limit, displayed notification, maximum limit of attempts reached. (Navigate to step 5)
- User details screen is displayed:
  - The user enters a new password, proceed to step 4
  - The user opts to cancel the process and is navigated back to the login screen
  - If a user does not update the password and clicks OK to continue, display a notification that a previous password cannot be reused
- The user has successfully updated their password and is now authorised to use the systems (End process)
- The forgot password function is disabled requiring the admin/implementor intervention to continue (End process)

Notifications:

- You are required to update your password to log in. Buttons: (1) OK
- Incorrect answer provided. You have <<number>> attempts remaining. Buttons (1) OK
- We have detected that you have used this password before. Secure your account by choosing a unique password. Buttons (1) OK

FIGURE 2 INITIAL LOG IN



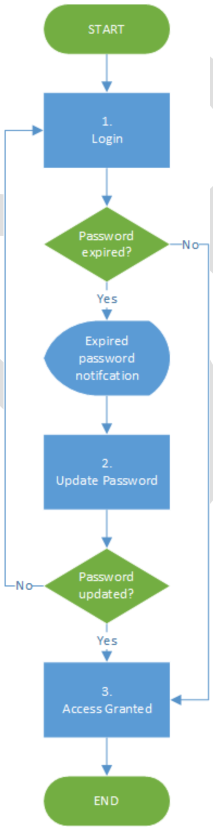
Process Steps:

- During login the system verifies if it is the users first login request
- If logging in for the first time, the system will display a notification advising that the password needs to be updated (navigated to step 2).
- End process if the user has a successful login history
- Display user details screen:
- After a successful password update proceeds to step 3
- If the user cancels the step, the system will close the screens and redirect the user to the login screen
- If a user does not update the password and clicks OK to continue, display a notification that a previous password cannot be reused
- The user has successfully updated their password and is now authorised to use the systems (End process)

Notifications:

- You are logging in for the first time with this account.
- You are required to update your password to continue. Buttons (1) OK
- We have detected that you have used this password before.
- Secure your account by choosing a unique password. Buttons (1) OK

FIGURE 3 EXPIRED PASSWORD



Process Steps:

- When logging in, the system verifies that the user password has expired.
  - If the password is still valid end process
  - If the password has expired display the expired password notification and navigate the user to user details screen
- User details screen is displayed with a prompt to update the password:
  - The user enters a new password to password to continue (step 4)
  - The user opts to cancel the process and is navigated back to the login screen
  - If a user does not update the password and clicks OK to continue, display a notification that a previous password cannot be reused
- The user has successfully updated their password and is now authorised to use the systems (End process)

Notifications:

- Your password has expired. You are required to update your password to log in. Buttons (1) OK
- We have detected that you have used this password before. Secure your account by choosing a unique password. Buttons (1) OK

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

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

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