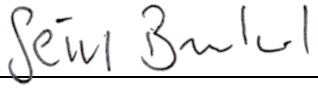
Standard Operating Procedure for User Access to Health Information Systems

Document Control:	Version 4.3
Prepared by:	Mr. Mahlatse Mokoena
Approved and signed:	Dr Sean Broomhead
	
Date:	04/12/2023

Contents

i) Abbreviations

API	Application Programming Interface
CEO	Chief Executive Officer
DHMIS	District Health Management Information System
GIS	Geographical Information System
HIS	Health Information System
HISP	Health Information Systems Program
HTML	Hyper Text Markup Language
NDD	National Data Dictionary
NDOH	National Department of Health
Postgres	PostgreSQL
SA	South Africa
SLA	Service level agreement
SMS	Short Message Service
SOP	Standard Operating Procedure
SQL	Structured Query Language
webDHIS	web-based DHIS

Background

The eHealth Strategy and the District Health Management Information Systems (DHMIS) policy provide the backdrop for the implementation of Health Information Systems (HIS) in the South African Health environment. The eHealth strategy places different structures and systems in the context of the larger eHealth environment. Even though some of these structures or systems will take some time to realise their intended purpose fully, it is nevertheless essential to put Standard Operating Procedures in place, which govern how access to Health Information Systems are managed, whether on a short-, medium- or long-term basis.

Thus, this document is not aimed at providing a long-term SOP for user management, as this will change as the eHealth environment develops, interoperability increases, and HIS databases develop over time.

The document is aimed explicitly at Health Information Systems and should be implemented in accordance with the ICT Information Security Policies of NDOH.

The use of OpenID

Industry innovations have developed rapidly over the last few years, and OpenID is one such innovation where a user gets issued one OpenID from an OpenID provider. Examples of such providers widely known are Google, Facebook, Twitter, LinkedIn, etc. The OpenID provider can be linked to systems such as online databases and act as a single login.

The benefit of OpenID is that a user has one Username and Password to log in to multiple systems and, therefore, is only required to remember the login details for one system. This is much preferred to users not remembering their login details and thus having to write these login details down where they can be accessible to other users.

Entities can register as an OpenID provider and control the issuing of OpenIDs to legitimate users only. The NDoH is actively exploring this option for controlling access to database systems. However, developing a fully-fledged OpenID with a registry that can link to all Health Information System databases will take some time.

The NDoH is also committed to ensuring that industry-standard user security measures are adhered to even during this SOP's short and medium-term phases.

Health Information system-specific user management

1. Introduction

Information security is one of the most important aspects of Health Information Systems and the National Department of Health, driven partly by changes in the regulatory environment and technological advances. Information security ensures that data and infrastructure are protected from risks such as unauthorised access, manipulation, destruction, or loss of data, as well as the unauthorised disclosure or incorrect processing of data.

2. Objective

The objective of the standard operating procedure (SOP) is to define the user access management control measures for webDHIS information, which would apply to the users employed by the National Department of Health, Provincial Departments of Health, and other stakeholders. This SOP seeks to ensure that it protects the privacy, security, and confidentiality of the departmental health institution information.

The main objective of this SOP is to provide the Department with best-practice User Access Management controls and procedures to assist the Department in securing its user access management procedure.

3. Purpose/Aim

This policy aims to ensure that the Department conforms to standard user access management controls to balance compliance, best practice controls, and service efficiency and mitigate risks associated with managing user access. This SOP supports the departmental Governance of the DHMIS Policy.

4. Scope of work

The User Access Management SOP has been developed to guide and assist the Department in aligning with internationally recognised best practice User Access Management controls and procedures. This SOP further acknowledges that the Department is diverse and, therefore, adopts the approach of establishing principles and practices to support and sustain the effective control of user access management in the Department.

The SOP applies to everyone in the Department, including its stakeholders. This SOP is considered crucial to the departmental operation and the security of routine health information systems.

The SOP covers the following elements of user access management:

- New user registration;
- Terminated user removal;
- User temporarily disabled;
- User multiple accounts;
- Temporary account;
- User permission/role change request;
- Reviewing user access permissions; and
- User and administrator activity monitoring.

Aspects relating to ICT security and operating system security controls are contained in the ICT Security Controls and ICT Operating System Security Controls policies.

5. Breach of SOP

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of SOP. All misconduct and/or breach of contract will be assessed by the Department and evaluated on its severity level. Appropriate disciplinary action or punitive recourse will be instituted against any user who contravenes this SOP.

6. Administration and responsibilities of SOP

The HIS Manager within the Department at the National, Provincial, District, and Sub-District levels is responsible for maintaining this SOP. The SOP must be reviewed by the HIS Steering Committee on an annual basis.

Manual creation, deletion, and changes of user accounts and privileges must be carried out by trained and authorised staff.

7. New user registration

i) User access to webDHIS is granted on a minimum permissions basis, meaning that every user should be allocated the minimum set of permissions required to perform their function adequately in the system.

ii) A formalised user registration process must be implemented and followed to assign access rights.

iii) All user access requests must be formally documented and uploaded, along with the access requirements, and approved by the applicant's manager using the user access request form. The template for this type of request can be found attached to this SOP in Annexure A. In cases where large numbers of users need to be registered, a CSV template approved by an appropriate manager may be used and uploaded instead of individual user registration forms.

iv) User access requests must be obtained from HIS personnel when registering a new user. The form must be sent to the line manager for access requirements to be requested (HIS may be consulted for advice). Once the requirements have been requested and signed off by the line manager, the form must be sent to the HIS department to check that relevant user permissions were requested and approved, following the activation of the user based on the specified requirements will be completed. The form must then be filled and uploaded for record-keeping purposes. User access must only be granted once approval has been obtained. The user access request form signature and the date must not exceed two weeks. The user access registration form can only be submitted once, meaning, should the user require account activation, a new form must be submitted reflecting the current date.

8. Termination or user removal

i) A formal user termination process must be implemented to disable access rights.

ii) All user termination requests must be formally documented and approved by duly authorised personnel. Access must be disabled immediately once authorisation has been obtained by the line manager.

iii) Terminated user requests must be obtained from HR or HIS on the termination of an employee's employment in their current position. The template for this type of request can be found attached to this SOP in Annexure C. The form must be sent to the HIS department/line manager for access revocation/termination to be signed off. Once access revocation/termination has been signed off, the form must be sent to the HIS department for approval and deactivation of the user based on specified requirements. The form must then be uploaded on webDHIS for record-keeping purposes.

iv) Users who have left their place of employment may no longer use their previously granted access rights to obtain/access or remove any information from their previous place of employment. The user may not be permanently removed from the system, as they may have records associated with their account.

9. User account suspended/disabled

i) All users are meant to at least access their webDHIS user account in a 90-day cycle, failing which will result in the account being suspended/disabled.

ii) To enable/activate the account, the user will be required to obtain and complete a user access registration form. The formal procedure must be followed; thus, the applicant's line Manager must sign the user access registration form and send it to the HIS department. The account will only be enabled/activated if all compulsory fields have been completed.

iii) The date on the user access request form and the signature must not be older than two weeks, i.e., 14 days.

iv) The user account will be enabled and notified upon receiving a completed user access registration form. The form must be uploaded to the system, meaning that the user will now have two registration forms available in the system.

v) Create user may not physically change the user's password. After enabling the account, the user should be informed to utilise the forgotten password functionality to recover their account.

vi) The user may not alter their permission/role when requesting to reinstate their account.

vii) Should the user request more permissions/roles than they previously had, then the user will have to be clearly documented in the user access registration form; otherwise, the account will be restored/enabled in its original form.

viii) All users auto-disabled will not require an access termination form unless expressly indicated otherwise.

ix) Auto-disabled accounts will be accompanied by either one of the auto-generated comments, 'Disable: Lastlogin old' or 'Disabled: never login'. The former comment will be inserted in case section item (i) applies whereby the active user has not login in more than 90 days. The latter will apply when the account has never been accessed in more than 90 days since its creation.

10. User multiple accounts

i) A users role must be directly linked to their function. If a user has multiple functions such as Superuser, Admin User, Create user, Data Capturer etc, they must have multiple roles and log in with the specific role to perform the said function.

ii) The Create User permissions does include permissions of other roles, specifically important is permissions to capture data because else they cannot assign capturing rights to data capturer users. However, this permission in the Create User Role does not permit Create Users to capture data. Should they be required to also capture data they require a specific Data Capturer role.

iii) Each account must have an access registration form, signed, approved, and uploaded to the webDHIS for easier access and record-keeping purposes.

iv) The account name must clearly be distinguishable from a standard user account if it is an additional account added to the existing primary user account.

v) Test accounts must all be inactive/disabled; these accounts were created during initial system configuration or troubleshooting during implementation, and as such, they are no longer required. The account should be deleted if possible, and if they have records associated, then disabled.

11. Temporary account

i) Part-time/temporary users will be given access to the system. Users such as the auditors assess the system and the other users from the National Department of Health Supporting partners.

ii) These users will be granted temporary access for the period which they specified in the registration form.

iii) A formal process will be followed, a user access registration form will be acquired from the HIS or the webDHIS instance homepage.

iv) The form will be completed and signed by the applicant's supervisor. The form will be sent to the HIS directorate at the DOH for further approval.

v) Upon approval, the access will be granted temporarily. The access will be terminated at midnight of the date agreed upon and documented on the user access registration form.

vi) More information may be requested, and access may also be denied.

vii) Should the user wish to extend their access, the user will have to formally request another access using another user registration form signed and approved by the user's line Manager and the HIS directorate at the DOH.

12. User permission/role change request

i) A formalised user access management process must be implemented and followed to adjust user access rights.

ii) All user access change requests must be formally documented, along with their access requirements, and approved by duly authorised and trained personnel.

iii) Access must only be granted once approval has been obtained by the respective line manager.

iv) User access change requests must be obtained from HIS on the change of a user's role or permissions. The template for this type of request can be found attached to this SOP in Annexure A.

v) The form must be sent to the line manager for access requirements to be signed off. Once the access requirements have been signed off, the form must then be sent to the HIS department for approval and adjustment of the user's access rights based on specified requirements. The form must then be filed and uploaded for record-keeping purposes.

13. General user access rights assignment

i) Generic Access rights include, but are not limited to:

a) Access dashboard role

b) The All Metadata user group if the user is employed within the Department of Health. If the user is employed by other organisations. In that case, their access rights for reporting should be limited to the organisation unit where they work and system dashboards should only be shared with Partner Groups as approved by NDOH.

c) Data output and analytic organisation units at the provincial level if the individual is employed within the Department of Health. If the user is employed by other organisations, their access rights should be determined on an organisation unit basis.

d) Access to internal messaging and email for password recovery and other messaging notifications set up within the instance.

ii) User access follows a "principle of least-privilege" approach, whereby all access is revoked by default, and users are only allowed access based on their specific requirements.

iii) The levels or degrees of access control to classified information are restricted in terms of departmental prescripts.

vi) Access rights are assigned to a group/role. A user may then be assigned to that group/role.

14. Reviewing user access and permissions

i) User access and user permissions must be reviewed every quarter (3 months) by the system user administrator at the various levels within the Department.

ii) On a monthly basis, HR must send a list of all terminated employees for that month to the HIS department. This list must be used to ensure that all terminated users have had their access revoked. Should one or more terminated users still have access to the instance, an investigation into the finding must be conducted.

iii) On a quarterly basis, the HIS Manager must review all users with access to the environment and assess their rights for appropriateness. All users' access should be reviewed in terms of user roles,

user groups, access to the organisation unit for capturing, and access to the organisation unit for reporting.

iv) All reviews must be formally documented and signed off by the HIS Manager, and the last review becomes the authoritative document on user access rights, superseding individual access control forms. Documentation must be kept for record-keeping purposes.

v) Any user information accessed by HIS Managers or their delegates may not be used for any purpose other than the review of user information. In this regard, the Protection of Personal Information Act protects the personal information of individuals, and reviewers should comply with the constraints laid out in that act.

15. Reviewing system administrator access and permissions

i) Administrator access must be reviewed every quarter (3 months) by the HIS Manager at the various levels within the Department.

ii) On a monthly basis, all terminated system administrator employees must have had their access revoked. Should one or more terminated users still have access to the instance, an investigation into the finding must be conducted.

iii) On a quarterly basis, the HIS Manager on various levels must review and sign off all system administrator changes to metadata.

16. User activity monitoring

i) The built-in system password expiry date function should be activated in all instances to ensure that users are required to reset their passwords every 90 days.

ii) The built-in notification to users of pending password expiry within 14 days should be activated so that users get a notification that their password will expire and have the opportunity to reset their passwords.

iii) Enable the automatic activation of the feature that restricts user access for 15 minutes following seven unsuccessful login attempts. The system permits up to five failed login attempts, granting access upon correctly entering the password on the fifth try. Should the password be incorrectly entered on the fifth attempt, the account is locked, with the user receiving a notification only on the seventh login attempt.

iv) Dormant accounts (the last password reset 90 days / last active 90 days) will be disabled automatically with a script on the server, and deactivations will be written to a log file and will be accessible via the Data Manager. Users who still require access must then request a re-activation of their user account using the prescribed User Permission Form in Annexure A.

v) All reviews must be formally documented and signed off by the HIS Manager. Documentation

must be kept for record-keeping purposes.

vi) All changes made to metadata by users with privileged accounts (Superuser) will be written to a log file, which should be reviewed by a supervisor monthly.

17. Security features of webDHIS

The National Department of Health, upon transitioning from the offline DHIS 1.4. version to a web-based DHIS system, the following security features, which control user access and user permissions within the system, were introduced.

The specific user security features of webDHIS include the following:

Area	User security feature
User Roles	• An extensive user permission framework within the database requires permissions to be granted to a specific user for every action or access to features within the system. This allows administrators of the system to control on a granular level which users obtain access to which features; • Provides the ability to set up User roles which define the permissions users have access to view and perform specific functions in the system;
Sharing via User Groups	• An extensive sharing framework where different objects e.g., datasets, data elements, indicators, tracker programs, etc. must be specifically allocated to user groups for a user to be able to see specific content in the system;
Passwords	• User security features include one-way encrypted storage of the user password – this means that the password cannot be decrypted even if accessed in the backend database tables; • Functionality can be activated to enforce reset of user passwords periodically depending on the setting selected; • Industry-standard password sensitivity – webDHIS requires a password with at least 8 eight characters, one UPPERCASE, one lowercase, one special character, and one number. • A setting to enable password retrieval, which is done securely via sending an email to the user to reset their password • The system will not allow the use of any of the 24 previously used passwords on a password change.
Create Users	• Web-API functionality related to users, which allows bulk importing of users, sending user invitations, etc.;

	• The ability to grant users access to roles is controlled by a specific role with necessary permissions allocated to users who should perform this function.
Managed User groups	• WebDHIS allows more granular user access control by allowing a user to manage other users who belong to a managed user group. This will enable the user to give users the same/fewer permissions than self, thus limiting the changes this user can make to other user's details;
User Security	• The User tables are not accessible via the SQL view interface in the webDHIS frontend thus, users cannot extract unauthorised user data from the system. Essential user management and control are managed via the frontend user interface or the web API;
Manage active users	• User administrators have the ability to deactivate users when they have become inactive or leave their current position of employment
Log files	• Extensive logs of all activities within the system allow retrospective auditing of actions performed by users and record logs of any errors occurring in the system and the reason for those errors.

18. webDHIS

In the South African webDHIS environment, the following principles will be followed for allocating permissions to users in different webDHIS instances:

Area	Principle
Admin user	WebDHIS instances do have an admin user, which is the fail-safe user, who can be used to access an instance that has become otherwise inaccessible. Admin usernames will be changed during the configuration of the instance to another uniquely generated username and stored in a Bitwarden database, which HISP/NDOH will keep. The admin user is not intended to login to a database regularly but will be used to access the database when all other user details have become inaccessible. If this username is not kept secure access to the instance may become inaccessible;
Superusers	Superuser access will be limited to dedicated Data Manager/s and their Supervisors who need to have access to the system to assist with configuration and support in the database (HISP will initially fulfil this role while Provincial and National level Data Managers are trained and mentored to take over this role);

	For metadata and data synchronisation configuration settings between webDHIS instances, a specific user is for metadata synchronisation via web API. These user details will be set up and maintained as system user password resets are required;
User roles	For running specific tasks on a regular basis on the instance which requires a password to access, a generic task scheduler username and password will be created and used exclusively for this purpose;
	The basic principle followed will be that a user will be allocated the minimum necessary permissions to perform the tasks which the user's job requirements demand them to perform on a specific webDHIS instance;
	A specific user may fulfil one role in one instance, and a different role in another instance and access will be determined according to the job requirements for that particular instance;
	Superusers can access all functionality within the database, but the use of certain permissions will be monitored through the requirement to maintain an Instance Management Document in accordance with the Instance Management SOP and through monitoring of Metadata edits through a log file accessible via a SQL view.
Role of NDD in managing metadata	In the (NDD), a robust user access system is implemented, ensuring that individuals are granted specific user roles tailored to their responsibilities. These roles empower users with the necessary permissions to access, create, and edit designated metadata. Users have the appropriate level of access and control over metadata relevant to their tasks within the NDD. To uphold the integrity and consistency of our metadata repository, all modifications and creations are subjected to a meticulous approval process.
Usernames	All webDHIS users must be registered with an individual Username identifying the specific user by username. The SA Naming convention for usernames is Firstname_Surname, and where the username already exists, an additional digit can be used to distinguish the username because webDHIS does not allow duplicate usernames. Certain users who would log in with specific user roles will add a short description of the role behind the particular user role e.g., the Superuser vs Data Manager user role for one individual will be distinguished by the role added to Name_Surname
Generic usernames	The only exceptions where generic usernames will be accepted are: • The compulsory admin failsafe username.

	• On mobile devices, users share/transfer mobile devices, and the mobile device uses webDHIS apps to capture data. In these instances, using a generic username for the device does not pose a user security login risk when transferring the device to another user because the user does not log into the frontend user interface via the app. It will prevent many costly administrative processes. • Usernames required for performing automated tasks such as running scheduled tasks or tasks that facilitate synchronisation between webDHIS instances or webDHIS and other Health Information Systems Software packages. • A list of such usernames will be maintained with a definite indication of why those are required.
Passwords	All webDHIS instance settings require users to change their password every 90 days. Administrators should activate the password expiry to 90 days and activate the notification setting to notify users 14 days before their password expires daily. Once a user's password was last reset 90 days ago, a form will automatically appear upon login where the user will have to enter the old password and new password to reset their webDHIS password. Once a user's password has been deactivated, a user with permission to edit user accounts will have to reactivate the user once an appropriate form has been completed.
	Users' inability to remember their passwords has created multiple requests for password resets, which is very time-consuming and could potentially require a full-time high-level person just to reset passwords on webDHIS. For an administrator to reset a user's password is also a security risk because the manager knows the user's password. Thus, the webDHIS functionality to reset passwords will be turned on, which enables the user to request a password reset on their username, which must be linked to a personal email address when the user registers. If the user does not have a valid email address linked to their account, they will not be able to receive the email sent by webDHIS to allow the user to reset their password.
	Users' inability to remember a password is not a reason to create a duplicate user account – the user should use the password retrieval functionality to retrieve a password or alternatively contact a user with permissions to Create Users or Database Manager to assist with manual resetting of the password. The required form should be completed to reset passwords.

	Users should not use web browser features that prompt whether to remember usernames and passwords as this would pose a risk if the computer is unattended that another user can login using the saved username and password.
	Users should have relevant security on Windows login in accordance with the NDOH IT Security policy, which states that the user's Windows login must be changed every two months and that users must use a screensaver password.
Approve user rights on the system	Access for individuals to webDHIS is controlled by Managers at specific levels approving the rights for a user to have access to required roles within the instance. This is managed on an instance-by-instance basis. The pdf form "webDHIS User Registration Form" (Annexure A example) customised for each webDHIS instance is completed and electronically signed by the applicant and electronically signed by the manager as defined in Annexure B. Note: The webDHIS User Registration Form will be customised as required to match the instance without it affecting the content of this SOP.
	Managers approving user rights on the system should consider the tasks a user needs to perform, understand the roles and what they allow a user to do, and only approve the minimum set of relevant roles for a user to perform their job optimally. As far as possible, the User Registration Form will indicate which roles are required for which tasks for the bulk of users. The pdf User Registration Form must be electronically signed by the User and the Manager and should not be edited again after signature by the manager.
Create users or Managed User groups	Users with Create user rights or Users who are able to manage Users via the Managed User groups functions should always check that the permissions requested and approved are correctly requested and approved and adhere to the guidelines for Creating users. If there is a discrepancy, the user and manager should be contacted for clarification. The authenticity of the electronic signature must be verified by the create user by verifying that the document was not changed after the signature was applied.

19. WebDHIS user registration configuration

All webDHIS instances should be set up with the following configuration settings:

Area	Configuration setting

User roles	Standardised User Roles are defined in Annexure D below. These user roles may need to be adapted from time to time, and the annexure for user roles should be kept up to date without updating that annexure to influence the SOP.
	Standardised allocation of permissions to User Roles according to Annexure D below. These permissions do change when new webDHIS functionality is released or during changes in the Core webDHIS code and thus must be adapted accordingly.
	The Superuser role must have the "ALL" permission allocated to it to add NEW permissions defined in the Core code to any user role.
Password change	A system-wide reset of password settings should be turned on, which enforces the periodic reset of passwords (at least once every three months). A user will have to reset the password three months after creation and then every three months after the last reset. There are some systems where this will be overridden for special circumstances, but those should be documented in the Instance Management Document for that particular instance.
Self-registration	Self-registration will be limited to the Training instance with the user role "Training User". This user has already been allocated certain common permissions that users use during training, e.g., dashboards, data capturing, validation, data approval, data user, sending messages, etc. The user is also allocated to view the whole provincial hierarchy, as training requires users to be able to see how data is displayed at different levels.

20. Backend Access to the Postgres SQL database

This section relates to system security and will be covered in detail in the Systems Security SOP, but access to the Postgres SQL backend tables will not be permitted at all on production instances. If any SQL views, SQL updates, or SQL delete statements are required on the backend database, they should be developed on staging instances via Postgres Remote, which will be limited to well-trained staff and monitored by Senior Database Managers. A change control process will be in place for specific SQL statements to be approved by a Senior Database Manager (HISP) before it is submitted to the Infrastructure Management responsible for Server hosting, maintenance, and security, who will run the SQL statements only if there is approval.

Scheduled SQL tasks, which can contain SQL functions or SQL scripts, must also be approved via the change control process before they are instituted on the instance.

Annexure A: WebDHIS user registration form (example)

health

Department:
Health
REPUBLIC OF SOUTH AFRICA

FS webDHIS Access - User Registration Form

New users that require access to the webDHIS, OR Existing Users that want to change/edit their current permissions, will have to complete this registration form. Kindly complete the required user information and upload the form onto the webDHIS system to which you are requesting access. ONLY after signoff and approval, will the user be created or edited.

webDHIS User Information:

* Compulsory Information that must be completed

For existing users, only specify/tick the changes/additional e.g. Orgunit, user role, data set. If Termination box is ticked, provide the termination date.	☐ New User ☐ Existing User ☐ Change Password ☐ Change/Addition of Data Set Access ☐ Change of Organisational Units Access ☐ Change/addition of user role ☐ Termination ☐ Restore user account Reason for restoring the account: Termination Date:
First name (in full)*	
Surname (in full)*	
Email Address*	
Position (eg. Data Capturer, Information Officer etc)*	
Place of employment*	
ID Number*	
PERSAL/Employee Number*	
Cell phone Number (eg. 082 123 1234)*	
Please specify the **Orgunit Parent** for Capturing (the user will have access to this org unit and all its children)*	
Please specify the **Orgunit Parent** for Reporting (the user will have access to report on this org unit and all its children)*	

Annexure B: Manager Permission table for access to webDHIS

The table below reflects the intended level of the manager who will grant permission for users to access the webDHIS system. These permissions are dependent on the specific user being trained and able to display the necessary skills when tested to perform this function.

Manager	Level of the Hierarchy for which to approve user access
Director General NDOH	Assign the password for the NDOH instance admin user to one responsible individual. Grant permission for access rights to NDOH Users Grant permission for provincial level Creates User role in NDOH instance. Based on the NDOH Service Level Agreement (SLA) - grant permission to the CEO HISP to allow HISP users access as Superusers/Data Administrator/Database Manager/Custom report programming in order for HISP to maintain the configuration of datafiles and troubleshoot any reported problems in support of the webDHIS implementation Based on User requests from other sources outside the National Department of Health, including the prescribed Data User Protocol and Data User agreement, NDOH can approve user access to webDHIS systems for specific reporting that can be shared with the user. Alternatively, NDOH can extract reports into Excel from webDHIS systems and provide this information.
HOD Province	Grant or delegate the power to provide permission for access rights to Provincial level users in Provincial and NDOH instance. Grant or delegate the power to provide permission for District level Create User level user in Provincial and NDOH instance
District Manager	Grant or delegate the power to provide permission for access rights to District level users in Provincial and NDOH instance. Grant or delegate the power to provide permission for Sub-district level Create User level in Provincial and NDOH instance
Sub-district Manager	Grant or delegate the power to provide permission for access rights to Sub-district level users in Provincial and NDOH instance. Delegated user to create Sub-district and Facility level users in Provincial and NDOH instance
Facility Manager	Sign permission for Facility level users
CEO HISP	Grant permissions for HISP staff to access webDHIS instances. Assign the ownership of the admin username to one responsible individual to be maintained for ALL instances on behalf of NDOH

Note: Any of the above may delegate this responsibility to another official with adequate skills to perform the required tasks

Annexure C: WebDHIS User Registration Process

Register as a webDHIS User.

Background

The purpose of this section is to describe the user registration process to ensure that webDHIS users are granted the correct and necessary permissions for the tasks which they are required to perform in the webDHIS. The webDHIS as an online system is vulnerable to actions performed by users. Therefore, until users are trained to perform specific tasks, access to production systems will be limited to the minimum permissions required for the user to perform the functions required in their regular day-to-day jobs.

In webDHIS, access to functionality is controlled by creating an individual as a user in the system and then allocating specific user roles to the individual who controls:

- Access to log into the system with a confidential Username and Password.
- Access to functionality is dependent on the permissions allocated to the user role/s to which the user has access.
- Access to data sets and/or programs which are allocated to the user.
- Access to a certain level in the orgunit hierarchy for capturing and reporting. (Note: Even if a user does not intend to capture data, a data entry orgunit must be allocated to the user as other functions, such as data approval, are also controlled by this allocation. If the user is not required to capture any data, the lack of allocated data sets and capturing roles will prohibit the user from actually capturing any data).

Registration of Users in webDHIS Systems

To gain access to a webDHIS system, users are required to complete the prescribed “webDHIS Access – User Registration Form” (see example in annexure). There are several ways to register users in the webDHIS, and this section aims to clarify the preferred method of registration by exploring the different methods of creating users.

Manual registration of users

A webDHIS user with permission to add other users can manually complete the user creation form and add a user to webDHIS. A user's rights to specific permissions need to be justified and approved. Therefore, a "webDHIS Access – User Registration Form" was developed to be completed by each user who has access to the webDHIS so that access can be approved before the creation of usernames. Although manual registration of users is possible, it is not the most desirable method as the username and password entered by the creator of the username must be provided to the user (usually by email), and this does pose some degree of security risk, especially in health facilities where multiple individuals have access to a single facility email address.

Sending user invitations

A user who can create users in the system can set up email invitations to users. They need to pre-define the user role and access. The user will then receive an invitation to register and will have the predefined access rights once registered. The user will receive an email with an invitation to register for security reasons. This is a viable option but is not ideal. It requires knowledge of the user roles and organisation unit access required and can be time-consuming and very technical to set up.

Allowing users to self-register

By far, the easiest way to add users to webDHIS is to allow users to self-register based on a system-wide pre-defined user role granted to self-registered users. This method allows the user to add his/her own username and password, which is then secured with the user only. The administrator who creates users can then subsequently edit the permissions granted to individual users.

In production systems, the self-registered user role will be granted absolute minimal user privileges. The user will only be able to send an internal message requesting user rights and upload the required "webDHIS Access – User Registration Form." With permission to create users, the administrator will then allocate revised access based on the uploaded approved form. The form will also be stored in the webDHIS system for future reference or auditing purposes.

For training instances, the self-registered user role will be changed to Training User with access to basic Aggregated and Tracker capturing functions, and validation and reporting functions, which are the permissions required by primary webDHIS users. This will allow users to register in Training instances and access these permissions on training databases without further permissions required.

Direct adding of users via web API

In certain scenarios, it is possible and advisable to add users directly into the system for example when creating user access for a specific mobile device that will be used to post data to the webDHIS. In this case, the device is added to the system rather than the user since the device must be referenced by e.g., a sim card number to be able to post data to the webDHIS. This technical solution requires advanced coding expertise, so it is not preferable.

The National Department of Health will employ any of the above methods to register users, but the bulk number of users will be registered using self-registration. Regardless of the method of user registration, a user should only have one username for any specific role they need to perform on the database. Re-registering for the purposes of a forgotten password is not permitted.

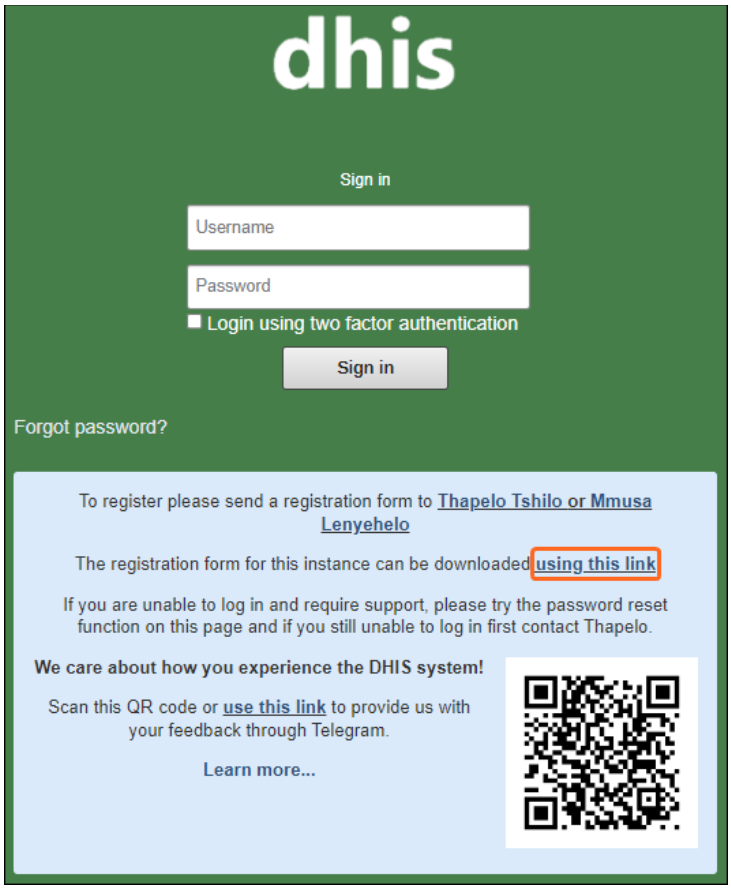
Current User Registration Process

The section describes in detail the steps to follow to register as a user on a webDHIS database.

Get the user registration form.

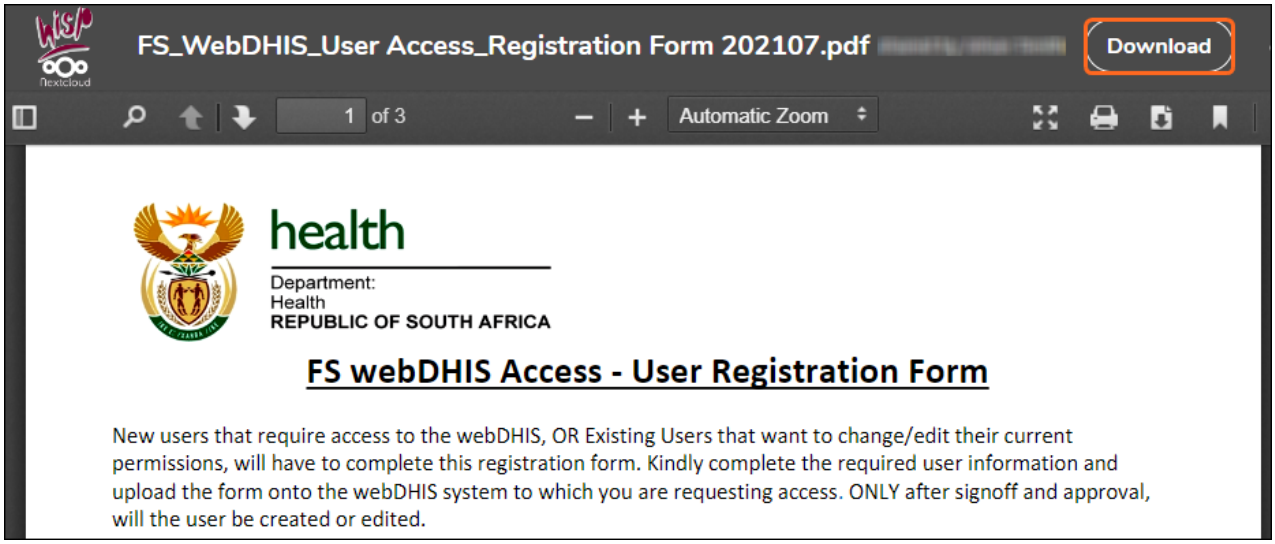
	Open Google Chrome.
	In your web browser, type the URL specific to your province or other database you want to access. **Note**: Each province has a specific URL – see examples below: • mp.dhis.dhmis.org • fs.dhis.dhmis.org

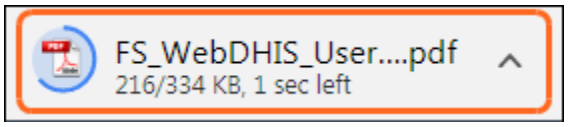
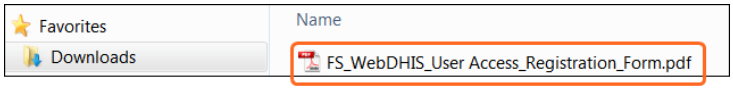
	• ec.dhis.dhmis.org • lp.dhis.dhmis.org • nw.dhis.dhmis.org There are other databases, such as: • pec.dhis.dhmis.org • ripda.dhis.dhmis.org



The Login screen displays.

To download the required form, click on the link **using this link**.



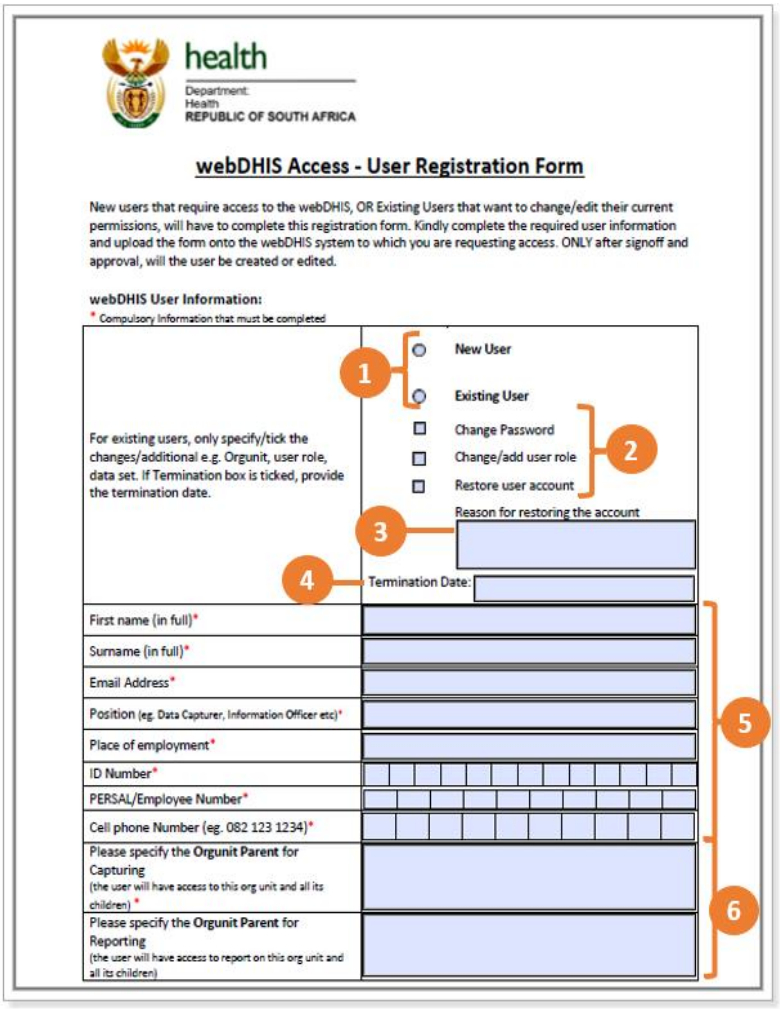
<table>
<tr><td colspan="2">The form opens in ownCloud – a file storage location.
Click on Download.</td></tr>
<tr><td> 
</td><td>The form will start downloading.</td></tr>
<tr><td> 
</td><td>Open the form from your Downloads folder so that it opens in Adobe Reader.</td></tr>
</table>

Fill in the user registration form.

The User Registration Form consist of three (3) pages:

1. Page 1 – New access request, existing access updates/changes, personal details and allocated Orgunits.
2. Page 2 - User roles, User groups and data sets for access.
3. Page 3 – Sign off page.

ALL 3 pages of the “webDHIS Access –User Registration Form” must be filled in.



health
Department:
Health
REPUBLIC OF SOUTH AFRICA

webDHIS Access - User Registration Form

New users that require access to the webDHIS, OR Existing Users that want to change/edit their current permissions, will have to complete this registration form. Kindly complete the required user information and upload the form onto the webDHIS system to which you are requesting access. ONLY after signoff and approval, will the user be created or edited.

webDHIS User Information:

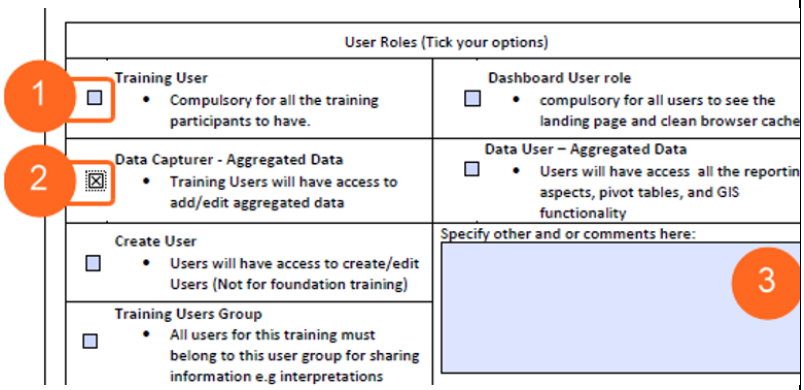
* Compulsory Information that must be completed

For existing users, only specify/tick the changes/additional e.g. Orgunit, user role, data set. If Termination box is ticked, provide the termination date.	1 ○ New User ○ Existing User 2 ☐ Change Password ☐ Change/add user role ☐ Restore user account 3 Reason for restoring the account 4 Termination Date:
First name (in full)*	
Surname (in full)*	
Email Address*	
Position (eg. Data Capturer, Information Officer etc)*	
Place of employment*	
ID Number*	
PERSAL/Employee Number*	
Cell phone Number (eg. 082 123 1234)*	
Please specify the **Orgunit Parent** for Capturing (the user will have access to this org unit and all its children) *	
Please specify the **Orgunit Parent** for Reporting (the user will have access to report on this org unit and all its children)	

5 6

Page 1:

1. Select either **New User** or **Existing User**.
2. If you are a new user continue to 4. If you are an existing user, choose options in 2, then continue.
3. Only complete by an existing user whose account has been **disabled** for whatever reason.
4. This is only completed for an existing user who will no longer use webDHIS. Insert **the last date the user will be using webDHIS.**
5. Complete your personal details.
6. Specify the **Orgunit parent** to which you belong.



User Roles (Tick your options)	
1 ☐ **Training User** • Compulsory for all the training participants to have.	☐ **Dashboard User role** • compulsory for all users to see the landing page and clean browser cache
2 ☒ **Data Capturer - Aggregated Data** • Training Users will have access to add/edit aggregated data	☐ **Data User – Aggregated Data** • Users will have access all the reportin aspects, pivot tables, and GIS functionality
☐ **Create User** • Users will have access to create/edit Users (Not for foundation training)	Specify other and or comments here:
☐ **Training Users Group** • All users for this training must belong to this user group for sharing information e.g interpretations	3

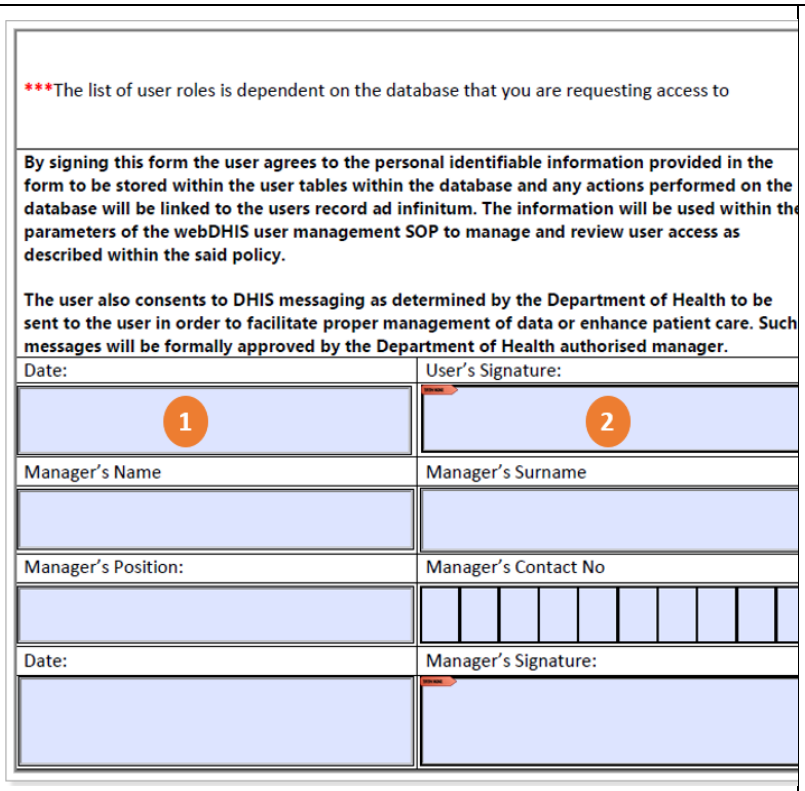
Page 2:

1. Click in the checkbox next to the user role/roles you require.
2. The checkbox is filled with an **X** when you click on it, indicating that you have chosen that option.

   Note: Please make sure your supervisor checks to see if the user roles you have selected are correct.

3. Specify any other user role required in the block provided.

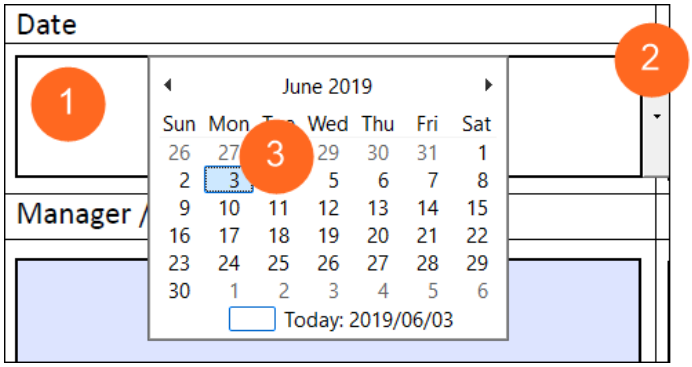
   If you have any additional comments, also type them here.



Page 3:

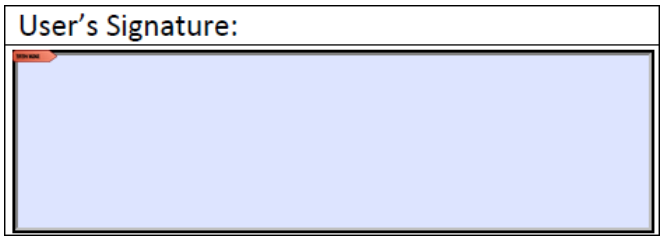
1. Enter the **Date**.
2. Attach your **User's Signature** (digital).

   These are described below.



1. Click in the **Date** field.
2. Click on the **dropdown arrow** that appears on the side of the Date field.
3. A calendar box will appear. Click on the required date.

Note: Today's date is the default setting.



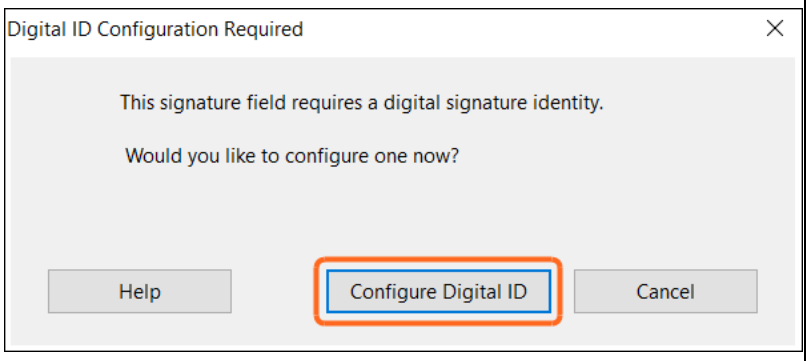
It is particularly important that this is the last field that you complete.

Click in the **User's Signature** field to insert your digital signature.

Note: Please note that the instructions below for creating/inserting a digital signature may vary slightly according to the version of Adobe Reader that you have installed on your computer. These instructions are for Adobe Reader DC.

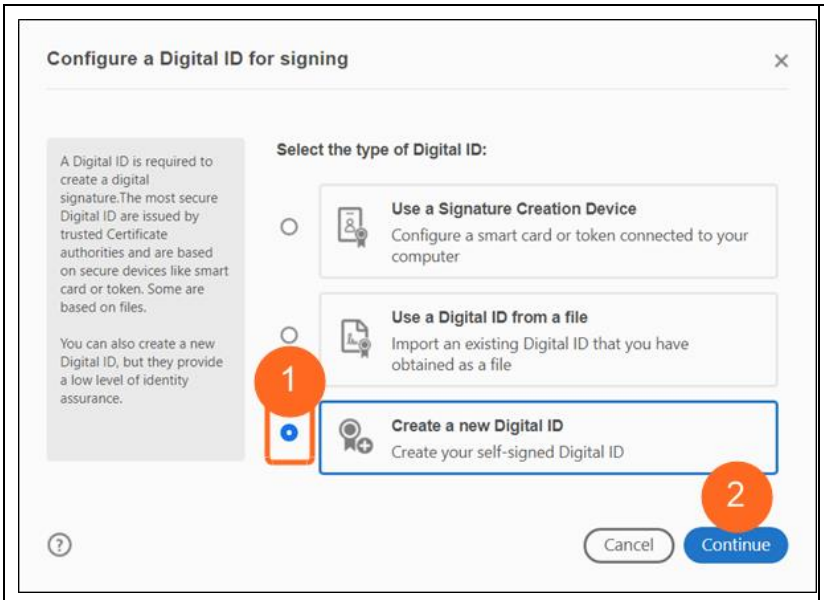
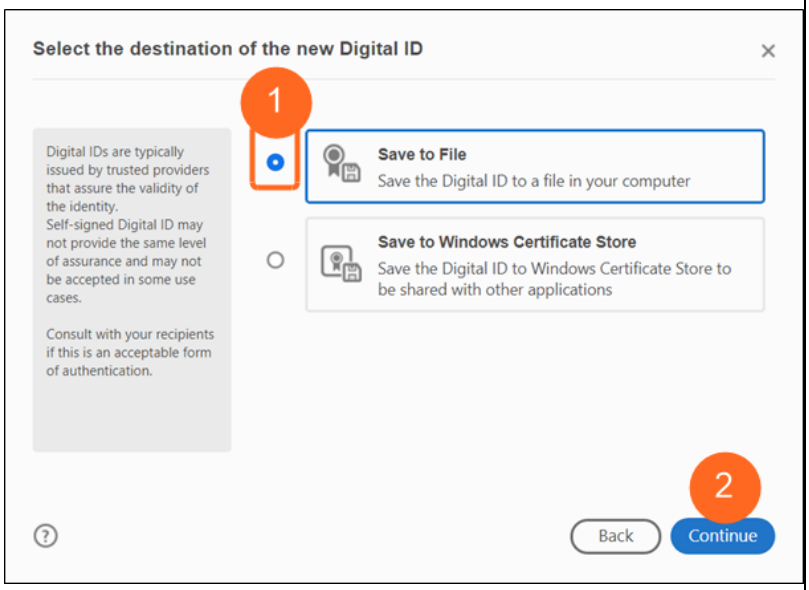
<table>
<tr>
<td> 
</td>
<td>If you have a digital signature:

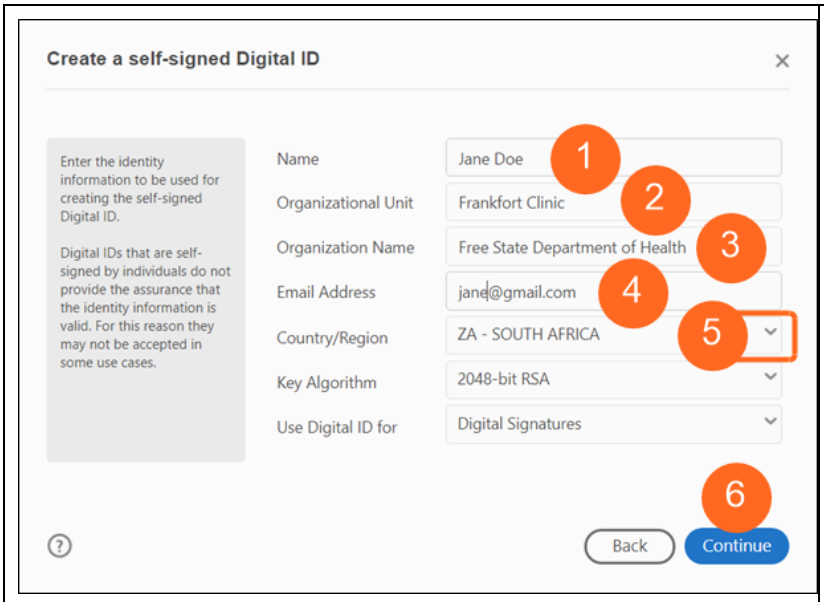
Select your signature (if there is only one signature, it will be selected by default).

Click on Continue.</td>
</tr>
<tr>
<td> 
</td>
<td>1. Enter the password for your digital signature.
2. Click on Sign.</td>
</tr>
<tr>
<td> 
</td>
<td>If you don’t have a digital signature:

You will be prompted to create one.

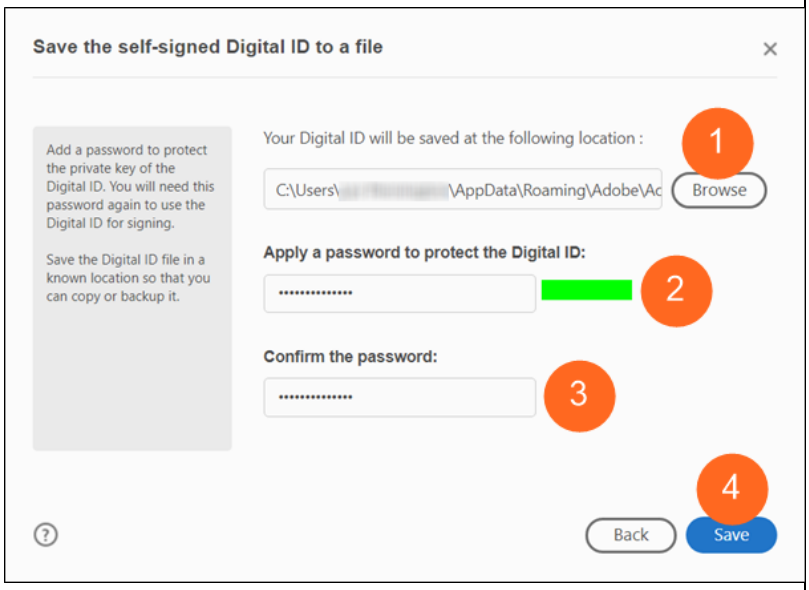
Click on Configure Digital ID.</td>
</tr>
</table>

<table>
<tr>
<td> 
</td>
<td>1. Click on the button next to Create a new Digital ID.
2. Click on Continue.</td>
</tr>
<tr>
<td> 
</td>
<td>1. The Save to File option is selected by default.
2. Click on Continue.</td>
</tr>
</table>



Enter your details as shown in the picture:

1. Enter your **Name** (first name and surname).
2. Enter the name of the **Organisational Unit** you are responsible for.
3. Enter the province you are operating in.
4. Enter your **Email Address**.
5. Click on the **Country/Region** dropdown arrow and select ZA - South Africa.
6. Click on **Continue**.



1. The file location for your digital ID will be displayed; you may change it or use the default location.
2. Enter a password for your digital ID.

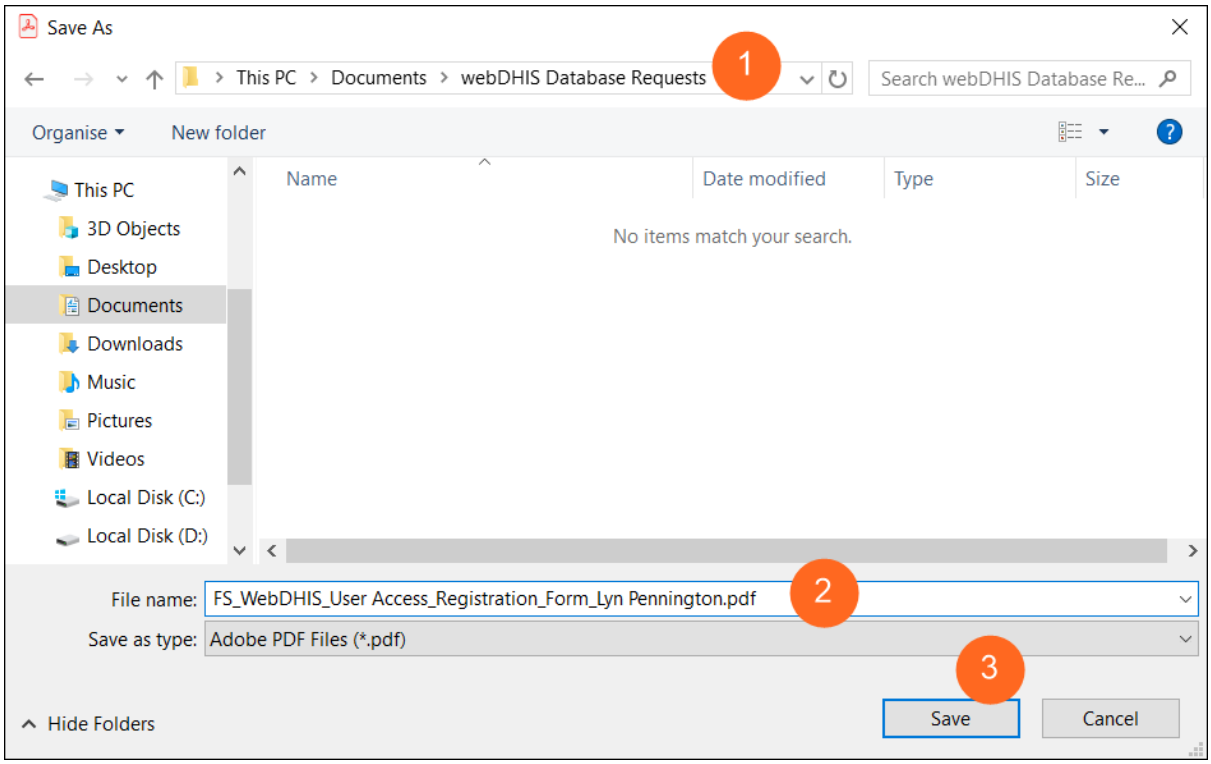
   TIP: The colour next to your password changes to show how strong your password is.

3. Enter the same password again.
4. Click on **Save**.

> Every time you use your digital ID, you will be required to enter the password, so please remember it!

1. Select your signature (if there is only one signature, it will be selected by default).
2. Click on **Continue**.

1. Enter the password for your digital signature.
2. Click on **Sign**.



You will be prompted to save your signed form.

1. Choose a suitable folder on your computer.
2. Rename the file to the following filename with the database prefix: *XX_WebDHIS_User Access_Registration_Form_Firstname Lastname*

   e.g**., FS_**WebDHIS_User Access_Registration_Form**_Lyn Pennington**

   <u>Note</u>:

   - The prefix is the part of the URL that comes before dhis in the URL name e.g., **ec**.dhis.dhmis.org.
   - Lastname is your Surname.
3. Click on **Save.**

1. Click on the **Signature Panel** icon.
2. Those who have signed the document are listed with a green tick to indicate the signature is valid.
3. Any unsigned fields are also shown.

The document will not be valid until all signature fields are completed – in this case, the supervisor must still sign.

Close the form and email it, or send it to your supervisor on a memory stick.

Your supervisor or manager will then check and approve the form by countersigning it.

Date:	User's Signature:
2021-01-28	Jane Doe Digitally signed by Jane Doe Date: 2021.01.28 06:08:01 +02'00'
Manager's Name	Manager's Surname
John (1)	Smith (2)
Manager's Position:	Manager's Contact No (4)
Line Manager (3)	0 8 4 5 6 5 6 8 9 5
Date:	Manager's Signature:
2021-01-28 (5)	John Smith Digitally signed by John Smith Date: 2021.01.28 (6) 47 +02'00'

The supervisor will complete the form by entering the following:

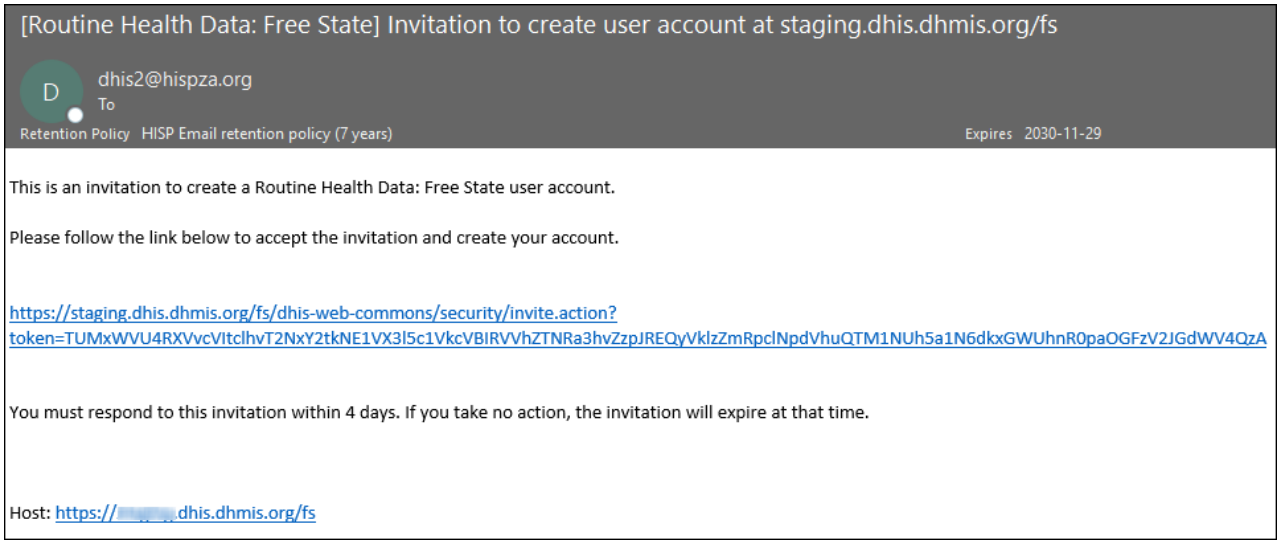
1. Name
2. Surname
3. Position
4. Contact Number
5. Date of signature
6. And by signing the form using the same instructions as above.

Note: The document may only be signed after checking that all the necessary fields are completed. The supervisor will return the form to the user for uploading to the database or may upload the form for the user.

	Rename the form that you have received back from your supervisor to append the date that you are sending it.

Complete the registration from the invitation.

You will receive an invitation via email. Click on the link to complete the registration and create your own password.



[Routine Health Data: Free State] Invitation to create user account at staging.dhis.dhmis.org/fs

D dhis2@hispza.org
To
Retention Policy HISP Email retention policy (7 years) Expires 2030-11-29

This is an invitation to create a Routine Health Data: Free State user account.

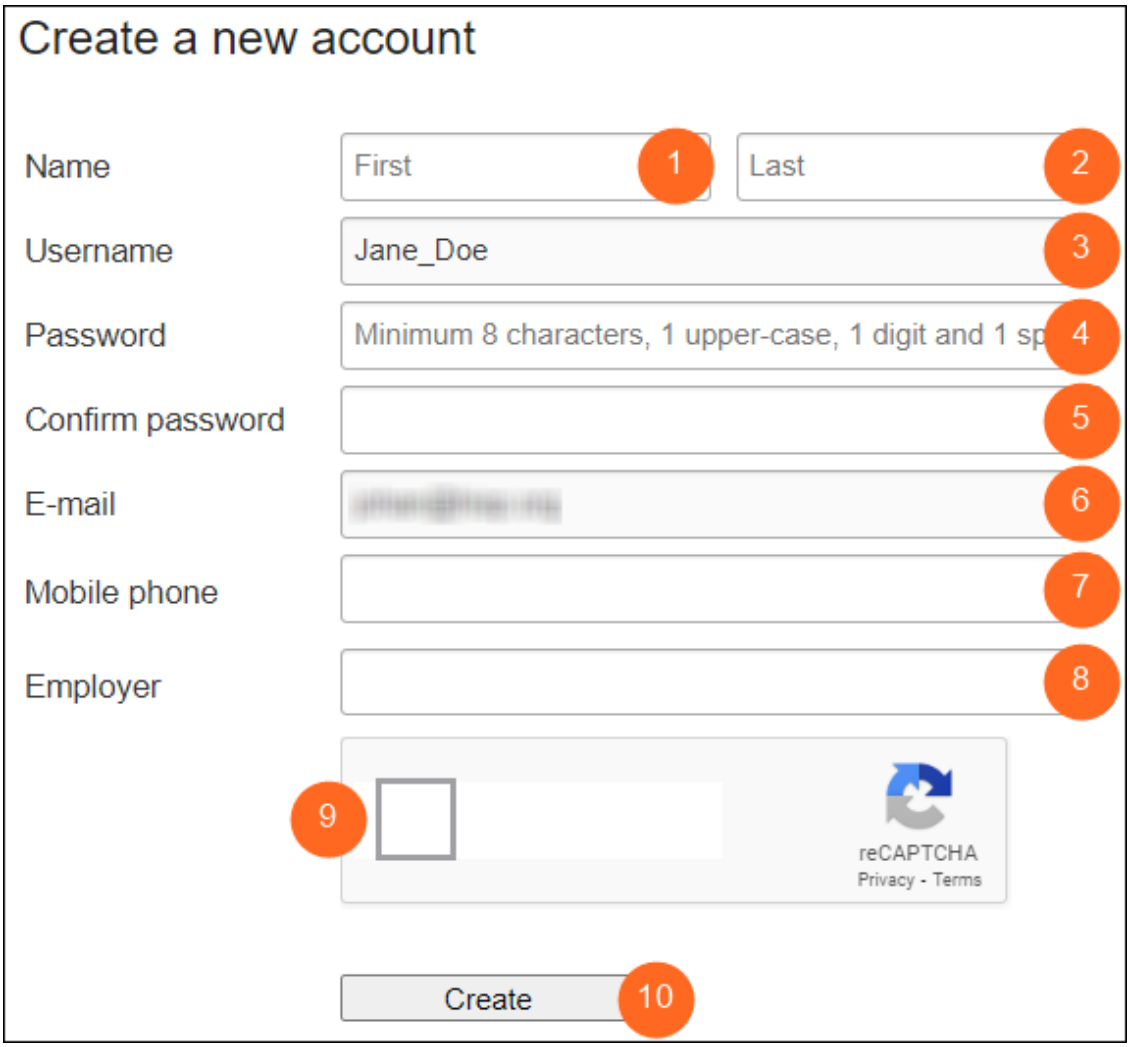
Please follow the link below to accept the invitation and create your account.

https://staging.dhis.dhmis.org/fs/dhis-web-commons/security/invite.action?token=TUMxWVU4RXVvcVItclhvT2NxY2tkNE1VX3l5c1VkcVBIRVVhZTNRa3hvZzpJREQyVklzZmRpclNpdVhuQTM1NUh5a1N6dkxGWUhnR0paOGFzV2JGdWV4QzA

You must respond to this invitation within 4 days. If you take no action, the invitation will expire at that time.

Host: https://[redacted].dhis.dhmis.org/fs

Once you click on the invitation link in the email, it will open the following page in the browser.



1. **Name/First**: Type your first name.
2. **Name/Last**: Type your last name i.e. your surname.
3. **Username**: Username will already be allocated.
4. **Password**: Enter your password.

Your password must:

- be 8-40 characters in length.
- contain at least one uppercase character, one digit and one special character (e.g., *, !) in addition to lowercase characters.
- not use generic words like system, manager, admin, password
- not contain any information from your account details e.g., your name, username, email address etc.
- not be one of the 24 passwords you have used previously.

You will get an error message if any one of these password rules is violated, and you will need to re-enter a valid password.

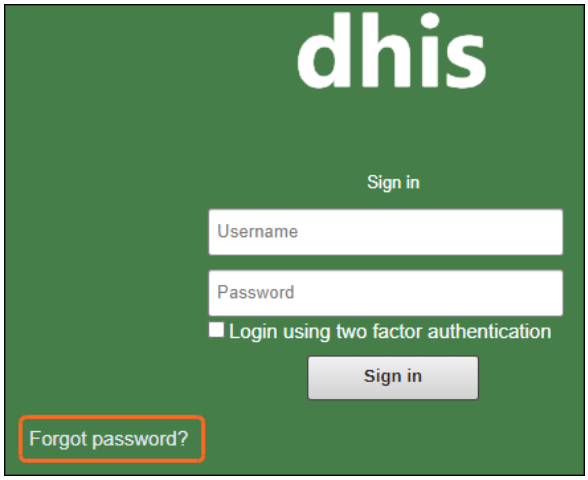
5. **Confirm password**: Type your password again, exactly as you entered it before.
6. **E-mail**: The email address that you provided on the form when you requested access and to which your invitation was sent will show here.

It is important that each user on the system is allocated their OWN departmental email account, not an account that all users share at a health facility.

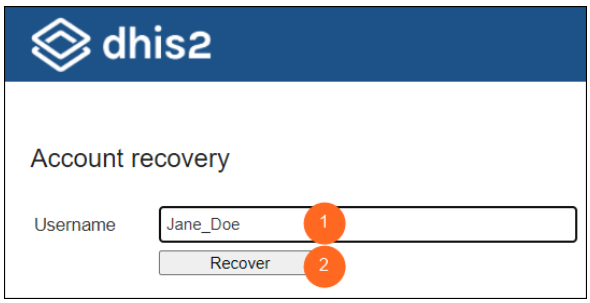
7. **Mobile phone**: Enter your mobile phone number.
8. **Employer**: Enter the name of your employer.
9. **I'm not a robot**: Tick the checkbox here to prove that you are not a robot.
10. When you have completed ALL the fields, click on **Create**.

Once you click on **Create**, you will be logged into DHIS.

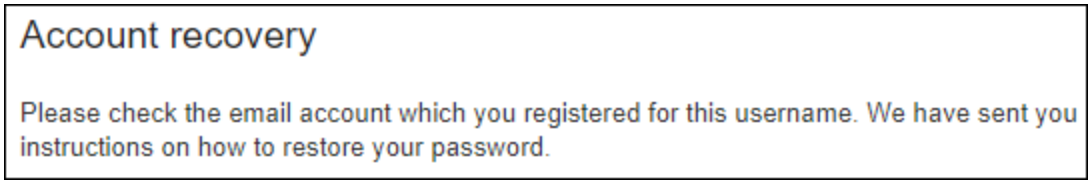
Password recovery



On the webDHIS Login screen, click on **Forgot password?** link



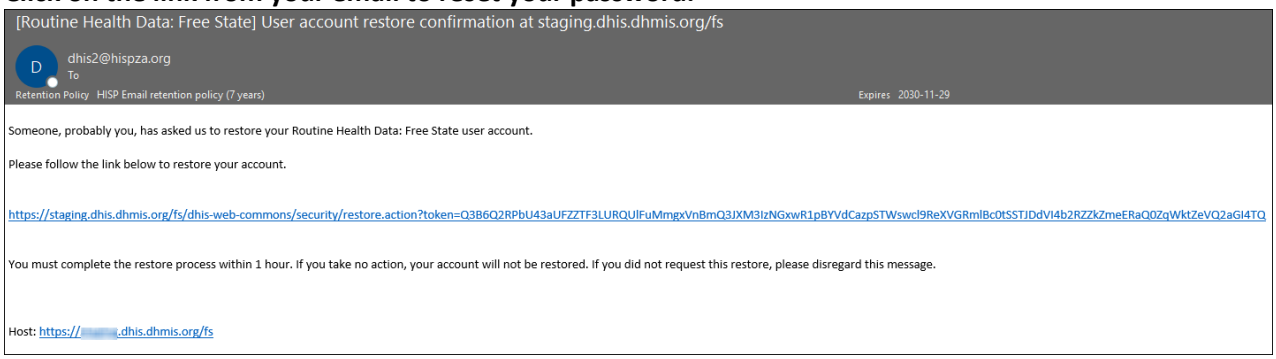
1. Type your username in the **Username** box.
2. Click on **Recover**.

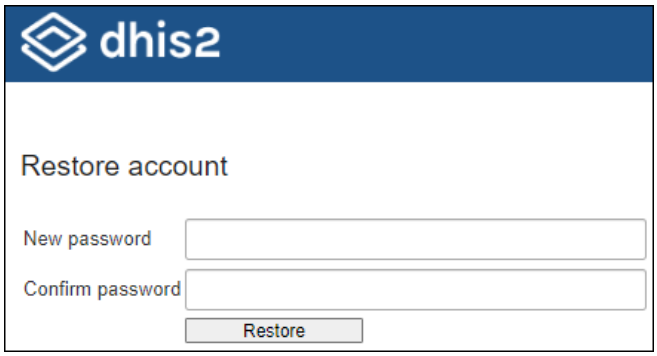


The account recovery message is shown.

Please check the email account that you used to create your profile on webDHIS – you should receive an email with a link to reset your password within 1 hour.

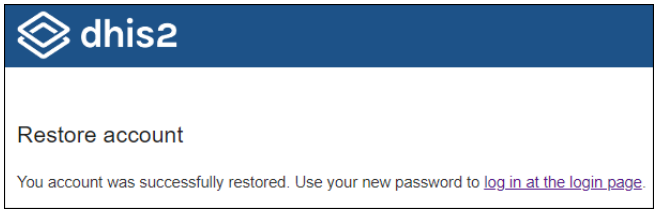
Click on the link from your email to reset your password.





Once you click the link, the subsequent page will open in the browser.

Type and confirm your new password.



A message indicates that your account has been restored successfully.

Please click the link to go back to the login page of the intended database and login with your new password.

Annexure D: List of webDHIS user roles and functions

The table below reflects the current user roles and the functions which each of these roles are able to perform in the webDHIS instance. Managers will have to take these roles and functions into account when approving the allocation of roles to users.

User Role	Description
Registration	This is the self-registration user role on production instances. The user only has access to one dashboard, which contains the forms necessary to request access to the instance. The role is unallocated once a user completes the user registration form, and illegitimate user registrations will be deleted
View Dashboard *	User role allocated to ALL users to access the Dashboard and Clear Browser Cache app. Without this role, a user would not be able to access the landing page of webDHIS
Send Messages	Access to send a message within webDHIS. If the users have email added under user, the message will also be sent via email
Data capturer - Agg	Access to capture aggregated data, add comments, run validations, and complete dataset on aggregated data
Data User - Agg	Access to create pivot tables, charts, GIS reports and dataset reports. Able to store these reports as Private favourites and add them to Own Private dashboard
Data capturer - Event	Access to capture event data (Event data is individual records without patient identifiable fields)
Data User - Event	Access to create pivot tables, charts, GIS reports, and dataset reports on event and tracker programs. Able to view events or Aggregated values. Able to store these as Private favourites and add them to the Private Dashboard
Data Capturer - Tracker	Access to capture tracker data - tracker data is individual records with patient-identifiable fields
Tracker Program Setup	Access to setup a Tracker Program (for Event or Tracker capture)
Message Config/Control	Access to configure/control mobile messages, which include the configuration of message text and scheduling of SMS according to specific triggers
Send SMS	Certain users may have access to trigger bulk SMS messaging based on the configuration settings above. Uses SMS bundle, which is purchased and loaded on the instance

Training User (activated as a self-registered user in Training instances only)	Access to Data Capturer (Agg, Event and Tracker) + Data User (Agg and Event) role, Run Validations, Data approval, Messaging, Dashboard
Data Validation	Access to generate Validations Rule Analysis
Approve data lower level	Access to accept and approve data at own and lower levels
Approval own level	Access to approve data at own level
Program Manager L1	Access to generate validation rule analysis reports, create private and public reports, data visualiser, GIS maps and add to the dashboard. Also, able to share favourites and share dashboards
Program manager L2	Access to generate validation rule analysis reports and create private reports, data visualiser, GIS maps and add to the dashboard. Not able to share favourites and dashboards
Import/Export Data	Access to import and export data
User Managed Groups	Access to manage user groups
Create User	Access to create users and allocate them the same user roles, datasets and orgunits as they have access to themselves. Also, have access to delete users with the same/fewer roles than themselves if those users are not linked to report favourites/data in the system already. Access to de-activate users no longer active
User Control	Access to control User Management in the system e.g., Create Roles, Create User Groups, Create User Managed Groups
Database Management	This user is the allocated Data Manager for the specific instance, taking responsibility for the overall integrity of the data and the instance functionality.
Database Management Training	This user is a Database Manager in training and will be allocated any subset of functions as training and mentoring progress, and when evidence exists that the DM can perform the function on training instances, it will be allocated on the production instance
Custom Report Programming	Access to create custom reports using HTML programming language
Database Admin	Database administrator who can perform higher-level administrative functions which require careful administration. High level of responsibility

NDD Metadata Control	These functions will not be allocated in production instances but exist on the NDD to control metadata (adding Orgunits, Data Elements, Indicators, Validation Rules, and all related objects such as Option sets, Category combinations, etc.)
Superuser	Access to ALL functionalities within the system. The admin user is, by default, a superuser and one/two more superusers need to exist in the system to ensure access to all functionality in the system