

DEPARTMENT OF HUMAN SETTLEMENTS

BAS USER ACCOUNT MANAGEMENT POLICY

Produced by:

Directorate: Financial Management

Contact persons: Ms T Sewedi

Contact numbers: 0183883601

E-mail addresses: tsewedi@nwpg.gov.za

TABLE OF CONTENTS

	Abbreviations	4
	Definitions	5
1.	Introduction	6
2.	Purpose of the policy	6
3.	Scope of application	7
4.	Objectives of the policy	7
5.	Policy principles	7
6.	Legislative mandate	8
7.	Roles and responsibilities	8
8.	Deliverables of the policy	9
8.1.	Limitation of SYSCON duties and handover	9
8.2.	User registration and creation of user ID	10
8.3.	Modification/change of user profile	11
8.4.	Removal and deactivation of user profile	11
8.5.	Activation and reset of user profile	12
8.6.	Review of user access rights	12
8.7.	Monitoring of user activities	13
8.8.	User profiles	13
8.9.	Amendment on code structure	13
8.10.	Logging of calls	14
8.11.	System overtime	14
8.12.	Verification of the validity system-level access granted to users	15
8.13.	Review of the System Controller's activities	15
8.14.	Password maintenance/control	15
8.15.	Disciplinary action	16
9.	The effective date of the policy	16
10.	Policy review	16
11.	Approval	17

ANNEXURES

- A BAS Security amendment form
- B BAS login procedure
- C Password reset procedure
- D Procedure to be followed when the password has expired
(both screens)
- E Procedure to be followed when downloading reports

ABBREVIATIONS

ABBREVIATION	FULL DESCRIPTION
AO	Accounting Officer
BAS	Basic Accounting System
FA	Functional Area
HOD	Head of Department
MEC	Member of the Executive Council
NWHS	North West Department of Human Settlements
PERSAL	Personnel Salary System
PFMA	Public Finance Management Act, Act 1 of 1999
POC USERS	Post-Audit Closure
SCM	Supply Chain Management
SITA	State Information Technology Agency
SYSCON	System Controller
USER ID	Unique Log-in number
WALKER	NW-Province-Procurement System

DEFINITIONS

Concept	Definition
Assistant/Sub-System Controller	Refers to an employee designated to assist the System Controller on the establishment of the Department to manage and control the general functioning of a specific transversal system
Chief Financial Officer	Refers to an employee designated in terms of Treasury Regulations 2.1.1 (or an employee acting in that capacity)
Department	Refers to the Provincial Department of Human Settlements, being a government department listed under schedule 1 of The Public Service Act
Line functionality/ Director	Refers to a senior manager (level 13 or above) or employee acting in that capacity
Sectional head/ Deputy Director	Refers to an employee responsible for overseeing and managing the operations of specific business activity or an employee acting in that capacity
System Controller	Refers to an employee designated on a fixed establishment of the Department to manage and control the general functioning of a specific transversal system
Transversal system	Refers to a computerized system that accounts for the financial and related transactions within the Departments. These systems include BAS, PERSAL and WALKER
User	Refers to an employee accessing a transversal system for the purpose of processing or authorizing transactions, updating or amending system data and extracting management reports from such system

1. INTRODUCTION

The effectiveness of the overall control environment for the Basic Accounting System (BAS) depends on the way various controls are applied in the Department. Where control measures are not applied and there are weaknesses in the environment, the effectiveness of the overall control environment may be impaired and may lead to increased risks. It is therefore necessary to ensure that measures are developed to ensure that all possible risks are properly mitigated; and this policy seeks to achieve such.

2. PURPOSE

The purpose of this policy is to provide a guideline on the minimum requirements users should adhere to when using, managing and administering transversal accounting systems within the Department

The aim of the policy is, therefore:

- 2.1. to identify and assess business impacts and risks that may arise as a result of control weaknesses;
- 2.2. to assist users of the Department with the application of the minimum requirements;
- 2.3. to provide guidelines to identify activities that are acceptable in terms of supervisory responsibilities and general limits of authority in terms of the financial functions of the Department;
- 2.4. to strengthen system security controls and ensure that Users access to systems and applications is appropriately restricted, segregated and monitored;
- 2.5. to limit access to personnel records to authorized users only;
- 2.6. to ensure that there is sufficient segregation of functions in the system; and
- 2.7. to provide certainty with respect to the treatment of financial matters undertaken within the Departments and ensure that management and employees assume their respective responsibilities, roles and duties.

3. SCOPE OF APPLICATION

The policy is relevant and applicable to all BAS users; it defines and prescribes the departmental prescripts, instruction, processes and procedures pertaining to the utilization, management and administration of Basic Accounting System within the Department for the purpose of restricting and monitoring access granted to users on the Basic Accounting System in order to prevent and detect a violation.

4. OPERATIONAL OBJECTIVES

This policy defines and prescribes Departmental prescripts, instructions, processes and procedures pertaining to the utilization, management and administration of the transversal financial system within Departments of Human Settlements for the purpose of:

- 4.1. emphasizing the culture of accountability for the utilization of Departments resources;
- 4.2. restrict and monitor access granted to users on the transversal financial system to prevent and detect unauthorized access;
- 4.3. ensuring that effective controls are communicated to the management and employees through a clear and comprehensive written document; and
- 4.4. provision of a formal set of Departmental prescripts, instructions, processes and procedures for compliance with the requirements of the PFMA, Treasury Regulations and other related statutes.

5. PRINCIPLES OF THE POLICY

This policy is underpinned by the following principles:

- 5.1. accountability;
- 5.2. compliance; and
- 5.3. transparency

6. LEGISLATIVE MANDATE

The following Acts and prescripts are central in defining departmental boundaries and areas of influence:

- 6.1. Public Finance Management Act 1 of 1999, Section 40(1)(a); and
- 6.2. Treasury Regulations Part 7 Section 17

7. ROLES AND RESPONSIBILITIES

7.1. System Controller

7.1.1. The System Controller is responsible for the effective, efficient, economical and transparent use of the system under his/her control which relates to the following:

- 7.1.1.1. All users granted access to the transversal system must be provided with a copy of this procedure manual and the user must acknowledge in writing the understanding of the contents of the procedure manual and ensure prescripts are adhered to.
- 7.1.1.2. First-time users of the system must be provided with formal training on General Principles of BAS as a prerequisite to other functional Areas (FA). Should a need arises for an official to perform task/s on the functional areas without formal training received on that FA, access can be granted on the condition that there is confirmation that the official has been provided with on-the-job training whilst awaiting formal training.
- 7.1.1.3. Users should be made aware of their responsibilities for maintaining effective access control, particularly the use of passwords and security thereof.
- 7.1.1.4. Evidence of the user activity must be kept to facilitate further investigation.

7.2. User

- 7.2.1. It is the responsibility of the user to safeguard his/her password at all times.
- 7.2.2. User should never share their password with any of their colleagues or supervisors.
- 7.2.3. If a user suspects that his/her password has been compromised, he/she must change the password immediately.
- 7.2.4. If a user suspects another user of utilizing his/her password, the matter must be reported to the System Controller immediately.
- 7.2.5. When the user is logged in to the system, he/she must ensure that if he/she leaves the office, he/she has logged off the system and also shut down his/her workstation whenever he/she leaves the office.
- 7.2.6. When maintenance is performed by technicians on the computer, a user should be present and witness all alterations (The user should never be logged in when maintenance is performed).
- 7.2.7. If a user takes leave, the matter should be reported to the System Controller in order to monitor the account for unauthorized access during the period of the leave(user must report before going on leave).
- 7.2.8. If a user is leaving the Department, the System Controller must be notified in writing by both user and supervisor to deactivate the account of the user. The user and supervisor must complete Annexure A and attach a report e.g. resignation letter, etc.
- 7.2.9. User must ensure that he/she logs on to the system at least once a week in order to keep his/her user profile active.
- 7.2.10. User may only obtain access to system functionalities directly related to the performance of his/her day-to-day activities.

8. DELIVERABLES OF THE POLICY

8.1. Limitation of SYSCON duties and handover

- 8.1.1. The System Controller is prohibited from participating in any transaction processing or authorization.
- 8.1.2. The System Controller is prohibited from creating user profiles with access to both transactional processing and authorization functions for the same functional area.
- 8.1.3. Should a System Controller become sick or take leave, the Director: Financial Management or the Chief Financial Officer must facilitate the handover process between the SYSCON and Assistant SYSCON. The same process should apply when s/he comes back from leave.

8.2. User registration and creation of user ID

- 8.2.1. A formal request (letter) by the user's Sectional Head, approved by the Chief Financial Officer for the creation of a new user profile should be forwarded to the SYSCON.
- 8.2.2. Access request form should be completed by the prospective user and authorised by sectional head or chief financial officer. The form should make provision for adequate details regarding user formation such as names, surname, PERSAL number, designation, section, region, contact details such as telephone number, cell number and email address must be provided. Other details required are:
 - 8.2.2.1. profile type/user level whether the user is a capturer or supervisor; and
 - 8.2.2.2. functions to be performed on BAS such that segregation of duties is achieved.
- 8.2.3. The following documents should be attached to the access request form:
 - 8.2.3.1. Annexure A: BAS Security Maintenance Form. Sections to be completed are (Part A and E only) and importantly Part E must be signed by Director: Financial Management, Chief Financial Officer or Supervisor. Form to be accompanied by the user's copy of his/her identity document.

- 8.2.3.2. The System Controller will then create a user profile as per Sectional Head's request and later on inform a user and relevant Sectional Head in writing or via email of the creation of a new user profile.
- 8.2.3.3. The System Controller must always keep the original request on file for a proper audit trail of access provided to the system.

8.3. Modification/change of user profile

8.3.1. The following documents must accompany the request for change/modification:

- 8.3.1.1. Annexure A: BAS Security Maintenance Form to be filled (Part A and E only) and importantly Part E to be signed by Director: Financial Management, Chief Financial Officer or Supervisor accompanied with a copy signed job description (if the change is permanent).
- 8.3.1.2. The period of access to the system will be effective e.g. if due to workflow changes whether this is permanent or temporary.

8.4. Removal and deactivation of user profile

- 8.4.1. Access is only granted to the users who are fully utilizing the system.
- 8.4.2. Should a user become inactive or dormant for a period exceeding one month, user profiles will be automatically deactivated by the system.
- 8.4.3. Where a user profile has been automatically deactivated by the system and the user fails to notify the System Controller within ten (10) working days from being deactivated, the System Controller will then permanently deactivate the user profile and notify the user in writing.
- 8.4.4. If a user terminates service with the Department or leave the Department due to transfer from or within the Department, resignation or death; the matter should be reported to the System Controller within thirty (30) days from the event so that the profile can be deactivated/removed.
- 8.4.5. A formal request (letter) by the user's Sectional Head, approved by Director/Chief Financial Officer stating the reason/s of termination; and

Annexure A: BAS Security Maintenance Form to be filled (Part A and E only) and forwarded to the System Controller. Importantly, Part E is to be signed by Director: Financial Management/Administration or Chief Financial Officer.)

- 8.4.6. Should a Sectional Head fail to inform the System Controller on time about termination of service by the user, he/she will be held accountable for any unauthorized transaction performed thereafter.

8.5. Activation and reset of user profile

- 8.5.1. Where a user wants to regain access to the system, the following should apply:
- 8.5.1.1. The user must write a letter to the System Controller stating reasons as to why he/she has not been using the system.
 - 8.5.1.2. A recommendation by the Sectional Head and approved by the Director: Financial Management or Chief Financial Officer.
 - 8.5.1.3. Annexure A: BAS Security Maintenance Form to be filled (Part A and E only) when resetting the password, and importantly Part E to be signed by Director: Financial Management, Chief Financial officer or Supervisor.

8.6. Review of user access rights

- 8.6.1. The review of users' access rights is required to maintain effective control over access.
- 8.6.2. User's access rights should be reviewed by the System Controller with the assistance of the users:
- 8.6.2.1. at least once per annum or;
 - 8.6.2.2. whenever there are changes to the organizational structure of the department such as transfer of functions or re-organizations; or
 - 8.6.2.3. whenever there is promotion, transfer and demotion of users.
- 8.6.3. A user should never have more than one user account on the system to perform different functions except for those who are performing Audit Closure i.e. POC users.

8.7. Monitoring of user activities

- 8.7.1. The System Controller should review user activity logs on the system on a monthly basis and provide a report to the Director: Financial Management or Chief Financial Officer.
- 8.7.2. The SYSCON must check the following:
 - 8.7.2.1. user name;
 - 8.7.2.2. User ID;
 - 8.7.2.3. login/out;
 - 8.7.2.4. failed logged in attempts;
 - 8.7.2.5. password change;
 - 8.7.2.6. password reset; and
 - 8.7.2.7. remarks/status at the end of the month.
- 8.7.3. Reports to be forwarded to the Director/Chief Financial Officer for comments if there are any and for sign-off.
- 8.7.4. System Controller to file signed user activity report for audit purposes.
- 8.7.5. Any discrepancy identified must also be brought to the attention of the supervisor.

8.8. User profiles

- 8.8.1. The System Controller shall maintain a file for all Users with documents supporting acceptance as user or changes to the user's profile

8.9. Amendment on code structure

- 8.9.1. The System Controller is the only authorized official to change or alter Departmental code structure.
- 8.9.2. Sectional Heads/users shall immediately when they become aware of a need to activate, amend or remove some of the segment details on the Department's code structure; inform the System Controller in writing to effect changes to the applicable code structure.

- 8.9.3. Should there be a need to change the objective or responsibility on BAS, a request letter from the relevant Programme Manager (Chief Financial Officer) should be sent to the Director: Financial Management or Chief Financial Officer. A copy of the existing and proposed structures to be attached to the request letter and this to be done through the assistance of the Budget Controller, and proposed changes to the code structure that impact the budgetary structure shall be recommended by the Budget Section.
- 8.9.4. Feedback regarding the amendments of the code structure shall be provided in writing to the Sectional Head/User/Programme Manager by the System Controller.

8.10. Logging of calls

- 8.10.1. A user must forward the e-mail to the System Controller outlining:
- 8.10.1.1. The reason/s of a call;
 - 8.10.1.2. The steps followed that led to the error; and
 - 8.10.1.3. Screen dumps/shots to be attached for easy reference
- 8.10.2. If the System Controller is unable to resolve the error encountered, he/she will log a call to National Treasury, through Provincial treasury; to obtain call number and then inform the user about the outcome of the call.
- 8.10.3. The sooner a user informs the SYSCON about the error, the better in order to avoid delays in terms of service delivery.

8.11. System overtime

- 8.11.1. The system is shut down at 17h00 daily to allow back ground batch run to take place uninterrupted
- 8.11.2. There is however, a need from time to time to keep the system available for users outside the normal working hours as follows:
- 8.11.2.1. Mon –Thu: between 05h00- 07h00 and 17h00-20h00;
 - 8.11.2.2. Weekends and Public Holidays 05h00 – 07h00 and 17h00- 20h00;
 - 8.11.2.3. Fridays: 05h00-07h00;

8.11.2.4. Or, any other times as dictated by the Provincial Treasury or SITA.

8.11.3. Should a need arises for a user to access the system outside normal working hours as specified above, a user should send a request in writing to the System Controller before 15h00 for overtime booking.

8.12. Verification of the validity system-level access granted to users

8.12.1. Sectional heads or supervisors of users must perform periodic checks to confirm that a user's current access to functions is commensurate with their current job description.

8.12.2. Where any discrepancies are detected, the System Controller must be informed and the profile amended accordingly.

8.13. Review of the System Controller's activities

8.13.1. The Director: Financial Management or Chief Financial Officer should review the activities of the System Controller at least on an annual basis or if there are changes in the workflow/profile to determine if the activities performed are in line with the job description.

8.14. Password maintenance/control

8.14.1. The system will prompt user to maintain his/her password once every 30 days

8.14.2. User may change his/her password at any time

8.14.3. The new password must meet the following complexity rules:

8.14.3.1. The password must be unique to the individual and should not be shared.

8.14.3.2. The password length must be at least seven (7) characters.

8.14.3.3. The password must be different from at least five (5) previous passwords.

- 8.14.4. The password must contain characters from three (3) of the following four (4) classes (or as outlined by the System Controller to the users so that it can be easily remembered), but in no specific order:
 - 8.14.4.1. Uppercase
 - 8.14.4.2. Lowercase
 - 8.14.4.3. Numerals
 - 8.14.4.4. Special characters
- 8.14.5. The password cannot contain spaces.
- 8.14.6. The password cannot contain non-anglicized characters.
- 8.14.7. Reference should be made to National Treasury prescripts/notices when released on password settings. If the requirements on the notices are more stringent than within this procedure manual, the notice should be applied and this procedure manual amended to reflect the change.

8.15. DISCIPLINARY ACTIONS

- 8.15.1. Where the System Controller, Assistant System Controller and users are found to have infringed on the requirements of these prescripts, disciplinary action should be considered in accordance with the Department's Disciplinary Code.
- 8.15.2. The Chief Financial Officer or his/her delegate must ensure that disciplinary action is taken within a reasonable period after an incident has been reported or alternatively as stipulated by the disciplinary code.

9. EFFECTIVE DATE

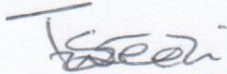
Policy will be effective from the date of approval of the document.

10. REVIEW

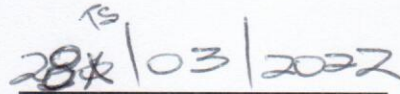
The policy shall be reviewed in conjunction with any amendments when a compelling need arises or every three years.

11. APPROVAL

Policy Developer:

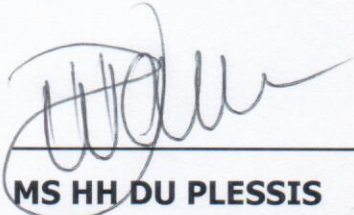


**MS T SEWEDI
CHIEF FINANCIAL OFFICER**

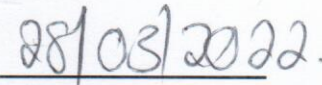


DATE

Recommendation:

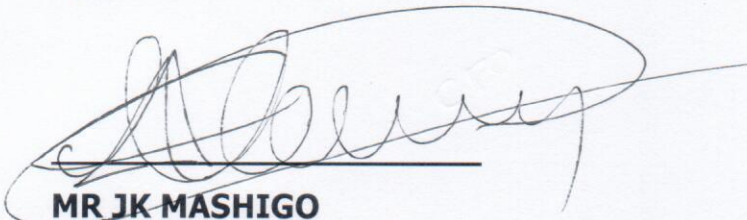


**MS HH DU PLESSIS
CHAIRPERSON:
DEPARTMENTAL POLICY OVERSIGHT COMMITTEE**

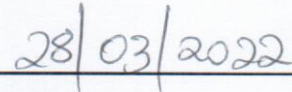


DATE

Approval:



**MR JK MASHIGO
HEAD OF DEPARTMENT**



DATE

ANNEXURE B

BAS LOGIN PROCEDURE

The following procedure prevails:

1ST SCREEN (REMOTE DESKTOP CONNECTION)

- 1 Go to Start
- 2 Click Remote Desktop Connection
The following default information will appear:
Computer: 10.145.145.201/2
User name: 1st characters of email address excluding @nwpg.gov.za
- 3 Click on connect

2ND SCREEN: LOG ON TO WINDOWS (MAINTAINED BY PROVINCIAL TREASURY)

- 1 User name: Enter your 1st characters of email address excluding @nwpg.gov.za (default)
- 2 Password: NB: (DO NOT TYPE ANY) This screen is maintained by provincial IT or the SYSCON
- 3 Click OK

3RD SCREEN: BAS (MAINTAINED BY THE SYSTEM CONTROLLER)

- 1 Double click on BAS_MMB
- 2 Foundation Environment Selection Screen will appear with HOSV5 as default (This depends on the version currently in use)
- 3 Click OK
- 4 On the User login Screen
 - 4.1 User ID (yellow field): Enter your User ID allocated to you by the SYSCON

- 4.2 Password (yellow field): Enter the password that you have created
- 5 Click OK
- 6 A message on the Welcome to the BAS version 3.0 screen will appear and make sure that you always read the message to check your password expiry date and last logged details
- 7 Click OK
- 8 The BAS main menu will appear and you will then access the functions allocated to you by the SYSCON

ANNEXURE C

PASSWORD RESET PROCEDURE

1 PROCEDURE TO BE FOLLOWED BEFORE THE SYSCON RESETS USER'S PROFILE

- 1.1 A User to fill in Part A only of BAS Security Maintenance Form (*ANNEXURE A*)
- 1.2 Screen dump reflecting error message to be attached on the form
- 1.3 A form to be forwarded to the Sectional Head for approval (Part E)
- 1.4 After approval by the sectional Head, a User should submit a form to the System Controller to reset password
- 1.5 The System Controller will then liaise with a User to check his/her availability before a password can be reset
- 1.6 User to log on BAS within a time specified by the SYSCON

2 PROCEDURE TO BE FOLLOWED AFTER THE SYSCON RESET USER'S PROFILE

Read the following steps carefully:

- 2.1 Follow steps on the 1st and 2nd screens of ANNEXURE B
- 2.2 On the 3rd screen, follow 1 to 4.1 of ANNEXURE B
 - 2.2.1 Press control C to copy User ID
 - 2.2.2 Place a cursor on password and press control V to paste
 - 2.2.3 Click OK. You will get a message "your password has been reset you are required to change it"
 - 2.2.4 Click OK
- 2.3 Go to field "Current password"
 - 2.3.1 Highlight User ID
 - 2.3.2 Press control C to copy User ID

- 2.3.3 Place a cursor on current password and press Control V to paste
- 2.4 Go to field "New password"
 - 2.4.1 Create a new password (comprising of 4 uppercase, 4 lowercase and 4 numbers or as prescribed by the SYSCON)
 - 2.4.2 Re-enter the password that you have entered (in 2.5(a) above. Ensure that the password is exactly the same.
 - 2.4.3 Click OK
- 2.5 **NB:** You will get the message clarified below indicating compliance with creation/changing of password. Read the messages carefully and Click OK right through until you see the BAS Main Menu

3 COMPLIANCE WITH BAS LOGIN PROCEDURES – CREATION/CHANGING PASSWORDS

- 3.1 The password must be unique to the individual and should not be shared
- 3.2 The password length must contain characters from four (4) of the following three (3) classes, but in no specific order:
 - 3.2.1 Uppercase (4)
 - 3.2.2 Lowercase (4)
 - 3.2.3 Numbers (4)
- 3.3 The password must not contain spaces.
- 3.4 The password must be different from at least five (5) previous passwords
- 3.5 Your new password will expire after 30 days
- 3.6 Your password will be automatically deactivated if inactive for a period exceeding 30 days
- 3.7 Should your password be reset by SYSCON, you will have to change it within a time specified or else it will be deactivated again
- 3.8 Your password will be deactivated after 3 unsuccessful attempts
- 3.9 Please note that by creating a password, it means that you are aware of and in compliance with BAS Login Procedures. These include:
 - 3.9.1 Demonstrating security behaviors and responsibilities
 - 3.9.2 Protecting password

- 3.9.3 Protecting BAS clients
- 3.9.4 Protecting data on computer

ANNEXURE D

1 PROCEDURE TO BE FOLLOWED WHEN THE PASSWORD ON THE 2NDSCREEN (MAINTAINED BY PROVINCIAL TREASURY) HAS EXPIRED

1.1 1ST SCREEN (REMOTE DESKTOP CONNECTION)

1.1.1 Go to start

1.1.2 Click remote Desktop Connection. The following Default information will appear:

1.1.3 Computer: 10.145.145.201/2

1.1.4 Username: 1st characters of email address excluding @nwpg.gov.za

1.1.5 Click on Connect

1.2 2ND SCREEN: LOG ON TO WINDOWS (maintained by Provincial Treasury)

1.2.1 Username: Enter your 1st characters of email address excluding @nwpg.gov.za (default)

1.2.2 Password: **NB: (DO NOT TYPE ANY)**. This screen is maintained by Provincial IT not SYSCON

1.2.3 Click OK

1.2.4 A pop-up message reading "Your password has expired you are required to change it" will appear

1.2.5 Click **OK** right through until you get the message that says (your password has been changed)

2 PROCEDURE TO BE FOLLOWED WHEN THE PASSWORD ON THE 3RDSCREEN (MAINTAINED BY THE SYSTEM CONTROLLER) HAS EXPIRED

2.1 1ST SCREEN (REMOTE DESKTOP CONNECTION)

2.1.1 Go to start

- 2.1.2 Click remote Desktop Connection
- 2.1.3 The following default information will appear:

Computer: 10.145.45.201/2

Username: 1st characters of email address excluding @nwpg.gov.za

- 2.1.4 Click on Connect

2.2 2ND SCREEN: LOGON TO WINDOWS (MAINTAINED BY PROVINCIAL TREASURY)

2.2.1 Username: Enter your 1st characters of email address excluding @nwpg.gov.za

2.2.2 Password: **NB (DO NOT TYPE ANY)** This screen is maintained by Provincial SYSCON

Click OK

2.3 3RD SCREEN: BAS (MAINTAINED BY THE SYSTEM CONTROLLER)

2.3.1 Double click on BAS_MMB

2.3.2 Foundation Environment Selection Screen will appear with HWKV4 as default (This depends on the Version currently in use)

2.3.3 Click OK

2.3.4 On the User Login Screen, perform the following steps:

2.3.4.1 User ID (**yellow field**): Enter your User ID allocated to you by the SYSCON

2.3.4.2 Password (**yellow field**): Enter the password that you have created

2.3.4.3 Click OK. Pop-up message "Your password has expired; you are required to change it", will appear

2.3.4.4 Click OK

2.3.5 Go to the field "Current password"

2.3.6 Enter the same password as the one entered in 2.3(d)(2) above

2.3.7 Go to field "New password"

2.3.8 Create a new password (comprising of 4 uppercase, 4 lower case and 4 numbers)

2.3.9 Re-enter the password that you have created on 2.3.2(b). Make sure that you enter the exact same password

2.3.10 Click OK

2.3.11 The BAS Main Menu will appear and you will then access the functions allocated to you by the SYSCON

ANNEXURE E

PROCEDURE TO BE FOLLOWED WHEN DOWNLOADING REPORTS

The following procedure must be followed:

1. Log on to BAS
2. Go to reporting
3. Click on Report Log
4. Click on the report that you want to download
5. Click on display
6. Click on download (at the bottom of page next to print) This message will appear:
"This report was not requested as download format. Are you sure you want to download it?"
7. Click OK
8. Path: type C:/BAS REPORTS file name: name your file e.g. EXCEPTION
9. Click OK
10. The report will be downloaded until you receive this message: (Report has been downloaded)
11. Click OK
12. Go to Start (BAS SCREEN- bottom left)
13. Double click my computer
14. Double click Local Disk (C)
15. Double click BASREPORTS folder
16. Search for your file e.g. EXCEPTION
17. Double click on the file
18. Click on Notepad (the file that you have downloaded will appear on the notepad)
19. Click OK
20. Highlight the whole file or alternatively Select ALL by pressing (Ctrl A)
21. Copy or alternatively press (ctrl C)
22. Minimize BAS Screen
23. Go to start (Windows)

24. Click on Notepad
25. Paste or alternatively press (ctrl V)
26. File your document
27. Then print your document using normal printer



ANNEXURE A - BAS SECURITY AMENDMENT FORM

A. DETAILS OF REQUESTING OFFICIAL:

Form with fields for SURNAME, NAME/S, USER ID, ID NO., PERSAL NO., SIGNATURE, DATE, SECTION, TEL. NO., E-MAIL ADDRESS, REGION.

I HAVE RECEIVED AND READ THE BAS USER ACCOUNT MANAGEMENT POLICY

B. REQUEST FOR CHANGES ON BAS:

Form with checkboxes for RESET BAS PASSWORD, WORKFLOW CHANGES, DE-ACTIVATE USER ID, REVOKE FUNCTIONS, ACTIVATE USER ID.

DESCRIPTION: (PLEASE PROVIDE ALL RELEVANT INFORMATION WITH REGARDS TO THE REQUEST)

Form with checkboxes for USER LEVEL (CAPTURER, SUPERVISOR, POC USER, BUDGET CONTROLLER) and FUNCTIONAL AREAS (PERIOD OPEN & CLOSING, RECEIPTS, DEBT, JOURNALS, BUDGET, DISBURSEMENTS, BANK SERVICES, ALLOCATIONS, ENTITIES, CONVERSION, PAYMENTS, INTERFACES, FINANCIAL REPORTING, OTHER).

DETAILED EXPLANATION:

C. REQUEST FOR CHANGES ON SEGMENT DETAIL: (Attach Supporting Documents)

Form with checkboxes for CREATE, AMEND, DELETE, RESPONSIBILITY, NON POSTING LEVEL, POSTING LEVEL, FUND, OBJECTIVE, PROJECT, ASSETS.

PLEASE NOTE: YOUR USERID'S AND PASSWORDS ARE STRICTLY CONFIDENTIAL! PER THE BAS USER ACCOUNT MANAGEMENT POLICY. YOU ARE NOT ALLOWED TO GIVE THEM TO ANYBODY ELSE. YOU ARE RESPONSIBLE FOR EVERY TRANSACTION WHICH TAKES PLACE UNDER YOUR USERID!!!!

I HAVE RECEIVED AND READ THE BAS USER ACCOUNT MANAGEMENT

SPECIFY THE STRUCTURE / DESCRIPTION:

PAYMENT, RECEIPT

D. SYSTEM RELATED REQUESTS:

Form with checkboxes for CAPTURE PRINTER, FAULTY REPORTS, OTHER, with sub-instructions.

Table with 2 columns and 6 rows for PROGRAM DIRECTOR APPROVAL (Surname & Initials, Persal number, Direct Tel number, Date, Signature).

Table with 2 columns and 6 rows for FOR SYSCON USE ONLY (Surname & Initials, Reference number, Feedback given, Date, Signature).