Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

Approval Date	28-11-2022
Periodical Review	Annually
Commencement Date	28-11-2022
Review Date	28 -11-2023

STANDARD OPERATING PROCEDURE: RESET PASSWORD ON ACTIVE DIRECTORY

TITLE OF SOP	Reset password on Active Directory
SOP Number	CIO-ICT-SA - 03
Purpose	To document the Standard Operating Procedure (SOP) for reset password process to assist the relevant ICT official in rendering the service and also the Departmental officials to be aware of the process.
Scope	The SOP applies to all officials involved in the process of password reset service within the Eastern Cape Department of Social Development.
Definitions and Acronyms	AD Active Directory ICT Information and Communication Technology IT Information Technology Ref Reference SCSM System Center Service Manager
Performance Indicator	**Number of ICT infrastructure support services rendered**

MA

STEP BY STEP GUIDE

RESET PASSWORD PROCESS

Nr	Task Name	Task Procedure	Responsibility	Time Frames	Systems and Supporting Documentation	Service Standard
1.	**Submit user Modify Form**	• User Fills in a downloaded User Modify Form. • All fields under **Personal Details** section are compulsory and no field left blank. • The user must Tick Password Reset option. • Sign the form and submit for Password Reset.	Applicant	20 Minutes	• Downloaded User Modify Form signed by applicant	Reset all password requests for the Departmental officials within one day of the receipt of the relevant document
2.	**Log a call**	• Log a call. • Assign a service request ref for the call. • Append the reference no to the user modify form. • Submit the form to the ICT Manager.	Desk	10 minutes	• Completely signed User Modify Form with a Ref. No	
3.	**Verify completed Active Directory User Modify Form**	• Receive completed Active Directory User Modify Form • Verify if it is properly filled in and signed accordingly.	ICT Manager	10 minutes	• Completely signed user Modify Form by all with a Ref. No	
4.	**Reset the Password**	• Login on AD system • Searches the user on AD system • Right click on the user object and click >Reset • Enter a random password to give to user and tick reset checkbox • File the reset request form • Notify the applicant about password reset by telephone.	ICT Manager	10 Minutes	• Completely signed User Modify Form with a Ref. No • Filed reset request form • Call used to inform the requester	
5.	**Update the password**	• Update the password to own personal Preference on the receipt of password reset. • Ensure that the following are catered when updating the password ➢ Minimum of 8 characters in length	Applicant	10 minutes	• Computer generated password • Updated password reset.	

MA

<table>
<tr><th colspan="7">STEP BY STEP GUIDE</th></tr>
<tr><th colspan="7">RESET PASSWORD PROCESS</th></tr>
<tr><th>Nr</th><th>Task Name</th><th>Task Procedure</th><th>Responsibility</th><th>Time Frames</th><th>Systems and Supporting Documentation</th><th>Service Standard</th></tr>
<tr><td></td><td></td><td>➢ At least one alphabetic and one numeric
➢ Different from the previous
➢ Password not to be the same as logon username
➢ Password must contain both upper and lower case characters
➢ Ensure that the password is not based on information that is easily obtainable (license plate, identity number, telephone number or child name)</td><td></td><td></td><td></td><td></td></tr>
</table>

MA

LEGISLATION REFERENCES

Document Name	Document or section extract description
Department of social Development Password policy 2021	To provide guidance on creation of strong passwords, the protection of those passwords and the frequency to change password in the Department.
Department of social Development Access Control policy 2021	To provide policy guiding framework on the processes and procedures on granting of access to the Department's information assets.
Protection of Personal Information Act No.4 of 2013	Section 13 Collection for specific purpose states the following: • Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. • Steps must be taken in accordance with section 18(1) to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of section 18(4) are applicable.
	Section 14 Retention and restriction of records states the following: 14.(1) Subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless— (a) retention of the record is required or authorised by law; (b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities; (c) retention of the record is required by a contract between the parties thereto; or (d) the data subject or a competent person where the data subject is a child has consented to the retention of the record. Records of personal information may be retained for periods in excess of those contemplated in subsection (1) for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes. A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must— (a) retain the record for such period as may be required or prescribed by law or a code of conduct; or (b) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record. A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2). The destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form. The responsible party must restrict processing of personal information if—

MA

Document Name	Document or section extract description
	(a) its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information; (b) the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof; (c) the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or (d) the data subject requests to transmit the personal data into another automated processing system.

MA

RISKS

Risk Name	Risk Description	Probability (H / M / L)	Impact (H / M / L)	Control Description	System / Manual
Down network or Servers	Down network or Server result in delay of password reset	L	L	Keep Servers and Network up almost all the time by network and server administrators.	System

MA

AUTHORIZATION

Designation:	Name:	Comments:	Signature	Date:
Recommended By: Director	T.M. Vazi			07/11/2022
Recommended by: Acting CIO	M.E. Gazi			7/11/2022
Recommended by: DDG	Dr.N.Z.G. Yokwana	3rd time submission		24/11/2022
Approved by: HOD	M. Machemba	Approved		28/11/2022
Distribution and Use of SOP	All Departmental staff			

MA