Province of the EASTERN CAPE
SOCIAL DEVELOPMENT

STANDARD OPERATING PROCEDURE: PROVIDE SERVER

Approval Date		31-01-2023
Periodical Review		Annually
Commencement Date		31-01-2023
Review Date		31-01-2024

TITLE OF SOP	SERVER PROVISIONING
SOP Number	CIO-ICT-SA-04
Purpose	To provide the server for the need identified by the requester.
Scope	This serves to provide the Eastern Cape Department of Social Development with Test, POC and Production Servers as requested. These can be at the Provincial, Districts or Metropolitans offices.
Definitions and Acronyms	AD — Active Directory CPU — Central Processing Unit DC — Domain Controller iDRAC — Integrated Dell Remote Access Controller iLo — Integrated Lights-Out OS — Operating System POC — Proof Of concept RAM — Random Access Memory UPS — Uninterrupted Power Supply VM — Virtual Machine
Performance Indicator	Number of ICT infrastructure support services rendered

MA

STEP BY STEP GUIDE
SERVER PROVISIONING

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard

1.	Identify Server need and complete the server provisioning form	• User Fills A Server Provisioning, Modification Form
		• The user indicates what the server is going to be used for
		• The user tells if the server creation priority is:
		  o **High** - Critical & Immediate
		  o **Medium** - Caution & Within A Week or
		  o **Low** - Caution & Within A Month
		• Indicate the number and size of Disks, RAM and CPU required.
		• Sign the filled form and submit for supervisor's recommendations.
			Applicant	10 Minutes	• Downloaded Server provisioning form
					• Signed server Provisioning Form
						Provide serves to all Departmental officials with approved request within 2 days

2.	Recommend server request	• Receive signed server provisioning form. • Recommend signed server provisioning form and submit to the Deputy Director: Data Center Management for approval.	Requester's Supervisor	10 Min	• Signed server Provisioning Form • Recommended Server Provisioning Form	
3.	Approve server request	• Checks for the availability of all the resources requested. • Approve creation based on the resource's availability. • Submit to Administrator-Data Center Management.	Deputy Director: Data Center Management	10 Min	• Recommended server Provisioning Form • Approved server Provisioning Form	

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
4.	Create the server	• Create the server by doing the following: i. Login the the vCenter ii. Highlight the host to create a VM iii. Select Action and New VM iv. Give your server a name v. Select Data Centre to create a VM vi. Select the host to create a VM vii. Select the Datastore to create a VM viii. Choose the Virtualization Platform ix. Choose the Virtualization OS and Version x. Assign resources as requested xi. Browse to Datastore ISO File xii. Select the server to install, connect xiii. VM Options and select Force BIOS setup xiv. Next and Finish xv. Go to your server and power on xvi. Boot Option and select CD-ROM, F10 and Yes xvii. Time and Currency Format and Install xviii. Select your Server OS, Desktop (Advanced) xix. Select the disk to install to and next to install xx. Once installed assign local Administrator password xxi. Create Local User for the requester and assign admin rights. • Inform the applicant about the created server.	Administrator Data Center Management	1 Hour	• Approved server Provisioning Form • Approved server Provisioning Form with created server	
5.	Acknowledge the receipt of the server	• Sign for the server to acknowledge that it has been created as requested.	Applicant	5Min	• Created server • Signed server creation acknowledgement.	

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
6.	Host the server	• Host server in a secure environment. • Server room must be specious to allow free movement. • Host server in a computer room with raised floor and free of water. • Ensure that Server room is free of flammable material. • Ensure that Server room have air conditioner and UPS. • Ensure that Servers have a proprietary embedded server management technology configured e.g. iLO or iDrac	Administrator Data Center Management	2 Hours	• Server room • Created server • Hosted server	

7.	Monitor and report on performance of created server	• Monitor and maintain servers to operate at peak performance.
		• Ensure that servers are always in warranty.
		• Make sure servers are always connected to the network.
		• Connect remotely to servers to check health status.
		• All default password to be changed to domain passwords
		• Fix hardware and OS problems a server might be experiencing.
		• Conduct a scheduled server room site visits for preventative maintenance.
		• Verify server fault lights, server room temperature, UPS status, any water on the floor, and if the server room is still secure during these visits.
		• Conduct ad hoc site visits should there be server problems which need physical intervention like changing faulty hardware, unable to connect remotely to the server, etc
		• Compile monthly report on the following:
		  ⮞ Visited sites.
		  ⮞ Encountered server room issues, resolved, and not resolved issues
		• Sign and present in a directorate meeting.
			Administrator Data Center Management	1 day	• Created server
					• Site visit Attendance register
					• Site visit report	

MA

Document Name	Section Description or Document Description

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
	
	2. 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.
	
	3. 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
	
	4. 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).

MA

Document Name	Section Description or Document Description
	5. 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. 6. The responsible party must restrict processing of personal information if— (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. 7. Personal information referred to in subsection (6) may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest. 8. Where processing of personal information is restricted pursuant to subsection (6), the responsible party must inform the data subject before lifting the restriction on processing.
Minimum Interoperability Standards Framework for Government Information Systems 2017	To describe open system standards that will ensure minimum level of interoperability within and between IS/ICT systems that are utilized in government, industry, citizens and the international community in support of E-government support systems.

RISKS

Risk Name	Risk Description	Probability (H / M / L)	Impact (H / M / L)	Control Description	System / Manual
Down Servers or Network	Down Servers or Network lead to no access to departmental systems	L	H	Keep Servers and Network up almost all the time. Keep Servers in secure server rooms	Manual

MA

AUTHORIZATION

Designation:	Name:	Signature:	Date:
Recommended By: Director-	T.M. Vazi		07/11/2022
Recommended by: Acting CIO	M Gazi		
Recommended by: DDG	N. Yokwana		7/11/2022
			06/12/2022
Approved by HOD	M. Machemba		31/01/2023
Distribution and Use of SOP	All Departmental staff		

MA