



Approval Date	08-11-2022
Periodical Review	Annually
Commencement Date	08-11-2022
Review Date	08-11-2023

**STANDARD OPERATING PROCEDURE: MODIFY SERVER**

<b>TITLE OF SOP</b>	Server Modification	
<b>SOP Number</b>	CIO-ICT-SA-05	
<b>Purpose</b>	To provide the server for the need identified by the requester.	
<b>Scope</b>	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 Metropolitan offices.	
<b>Definitions and Acronyms</b>	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
<b>Performance Indicator</b>	<b>Number of ICT infrastructure support services rendered</b>	

**STEP BY STEP GUIDE  
SERVER MODIFICATION**

Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
1.	<b>Complete Server modification request form</b>	<ul style="list-style-type: none"> <li>User Fills A Server, Modification Form and tick the required option.</li> <li>Specifies impact on users.</li> <li>Indicate the identified risks in the change including a review of reporting, security, user training, system interfaces and backups.</li> <li>Sign the form and submit for supervisor's recommendations.</li> </ul>	Applicant	10 Minutes	<ul style="list-style-type: none"> <li>Downloaded server provisioning modification request form</li> <li>Signed Server Modification Request Form</li> </ul>	Provide services to all Departmental officials with approved request within 2 days
2.	<b>Recommend Server modification request form</b>	<ul style="list-style-type: none"> <li>Receive signed server modification form.</li> <li>State if the mitigation options have been considered like Backup Roll Back Options.</li> <li>Specify testing required prior to placement into production if required.</li> <li>Recommend signed server modification form and submit to the Deputy Director: Data Center Management for approval.</li> </ul>	Requester's Supervisor	10 Min	<ul style="list-style-type: none"> <li>Signed Server Modification Request Form</li> <li>Recommended Server Modification Request Form</li> </ul>	
3.	<b>Approve Server modification request form</b>	<ul style="list-style-type: none"> <li>Checks for the availability of all the resources requested.</li> <li>Approve modification based on the resource's availability.</li> <li>Submit to Administrator-Data Center Management.</li> </ul>	Deputy Director: Data Center Management	10 Min	<ul style="list-style-type: none"> <li>Recommended Server Modification Request Form</li> <li>Approved Server Modification request Form</li> </ul>	
4.	<b>Modify the server</b>	<ul style="list-style-type: none"> <li>Modify the Server as per request.</li> <li>Inform the requester once the server is modified accordingly.</li> </ul>	Deputy Director: Data Center Management	1 Hour	<ul style="list-style-type: none"> <li>Approved Server Modification request Form</li> <li>Approved server Modification request Form with modified server</li> </ul>	
5.	<b>Acknowledge the receipt of the server</b>	<ul style="list-style-type: none"> <li>Sign for the server to acknowledge that it has been modified as requested.</li> </ul>	Applicant	5 Min	<ul style="list-style-type: none"> <li>Approved server Modification request Form showing Modified server</li> <li>Signed Server modification acknowledgement</li> </ul>	

**REFERENCES (LEGISLATION, POLICIES, PROCEDURES, LEGISLATION & OTHER DOCUMENTATION (i.e. SOPs))**

Document Name	Section Description or Document Description
Protection of Personal Information Act No.4 of 2013	<p>Section 13 Collection for specific purpose states the following:</p> <ul style="list-style-type: none"> <li>• Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.</li> <li>• Steps must be taken in accordance with section <u>18</u>(1) to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of section <u>18</u>(4) are applicable.</li> </ul>
	<p>Section 14 Retention and restriction of records states the following:</p> <ul style="list-style-type: none"> <li>• 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— <ul style="list-style-type: none"> <li>(a) retention of the record is required or authorised by law;</li> <li>(b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;</li> <li>(c) retention of the record is required by a contract between the parties thereto; or</li> <li>(d) the data subject or a competent <u>person</u> where the data subject is a <u>child</u> has consented to the retention of the record.</li> </ul> </li> <li>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.</li> <li>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— <ul style="list-style-type: none"> <li>(a) retain the record for such period as may be required or prescribed by law or a <u>code of conduct</u>; or</li> <li>(b) if there is no law or <u>code of conduct</u> 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</li> </ul> </li> </ul>

Document Name	Section Description or Document Description
	<ol style="list-style-type: none"> <li>4. A responsible party must destroy or delete a record of personal information or de-identify it as soon as <u>reasonably practicable</u> after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2).</li> <li>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.</li> <li>6. The responsible party must restrict processing of personal information if— <ol style="list-style-type: none"> <li>(a) its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;</li> <li>(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;</li> <li>(c) the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or</li> <li>(d) the data subject requests to transmit the personal data into another automated processing system.</li> </ol> </li> <li>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 <u>person</u> in respect of a <u>child</u>, or for the protection of the rights of another natural or legal <u>person</u> or if such processing is in the public interest.</li> <li>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.</li> </ol>
<p>Minimum Interoperability Standards Framework For Government Information Systems 2017</p>	<p>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.</p>



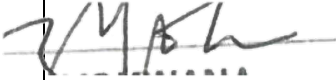

MA

## 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		07/11/2022
Recommended by: DDG	N.Z.G. Yokwana		08/11/2022
Approved by: Acting HOD	M. Machemba		09/11/2022
Distribution and Use of SOP	All Departmental staff		