



Approval Date	11 - 02 -2022
Periodical Review	Annually
Commencement Date	11 - 02 - 2022
Review Date	11 - 02 - 2023

STANDARD OPERATING PROCEDURE: MONITORING OF DAILY ONSITE BACKUPS AND REPLICATIONS

TITLE OF SOP	MONITORING OF DAILY ONSITE BACKUPS AND REPLICATIONS
SOP Number	CIO-ICT-BACKUP-001
Purpose	To document the standard operating procedure (SOP) for the daily monitoring of backups and replication schedules to assist the relevant ICT officials in rendering the service.
Scope	The SOP applies to all officials involved in the process of rendering monitoring of daily backups and replications services within the Eastern Cape Department of Social Development.
Definitions	Terms and Acronyms: Backup and Replication solution ICT: Information Communications Technology D.D: Deputy Director AD: Assistant Director Backup: information technology, a backup, or data backup is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event. Replication: performance of an experiment or procedure more than once.
Key Performance Indicator	Number of ICT infrastructure support services rendered

STEP BY STEP GUIDE						
MONITORING OF DAILY BACKUP JOBS ON VEEAM						
Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
1.	View Real-Time Statistics	<ul style="list-style-type: none"> Open the Backup & Replication view, in the inventory pane select Jobs, Last 24 hours or Running. In the working area, double-click the job. Open the Backup & Replication view, in the inventory pane select Jobs, Last 24 hours or Running. In the working area, right-click the job and select Statistics. 	AD: ICT Infrastructure	20 minutes	<ul style="list-style-type: none"> Backup notification e-mail of Backup Report Viewed Real-Time Statistics 	All mission critical server must be included in backup schedules, all backup scheduled jobs must be monitored daily basis, Backup and restore tests must be performed monthly and verified File level restores must be concluded within 48hrs.
2.	View Job Session Results	<ul style="list-style-type: none"> Open the History view. In the inventory pane select Jobs. In the working area, double-click the relevant job session. Open the History view. In the inventory pane select Jobs. In the working area, right-click the necessary job session and select Statistics. 	AD: ICT Infrastructure	20 minutes	<ul style="list-style-type: none"> Backup notification e-mail of Backup solution Report Viewed Job Session Results 	
3.	View Job Report	<ul style="list-style-type: none"> Open the Backup & Replication view. In the inventory pane, select Jobs. In the working area, select the necessary job and click Report on the ribbon. You can also right-click the job and select Report. 	AD: ICT Infrastructure	20 minutes	<ul style="list-style-type: none"> Backup notification e-mail of Backup solution Report Viewed Job Report 	
4.	View Job Session Reports	<ul style="list-style-type: none"> Open the History view. In the inventory pane, select Jobs. In the working area, select the necessary session and click Report on the ribbon. You can also right-click the necessary session and select Report 	AD: ICT Infrastructure	20 minutes	<ul style="list-style-type: none"> Backup notification e-mail Backup solution Report Viewed Job Report 	
5.	Provide first line support to resolve the error	<p>In case there is an error</p> <ul style="list-style-type: none"> Resolve the error using previous experience and knowledge (Disc space, configuration etc) Search for the error message on Google and other websites to find a solution. Try some of the Internet solutions that you think are relevant to the error. 	AD: ICT Infrastructure	1-3 days depending to the kind of an error	<ul style="list-style-type: none"> Resolved error 	

STEP BY STEP GUIDE						
MONITORING OF DAILY BACKUP JOBS ON VEEAM						
Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
		<p>In case of loss or corrupt files</p> <ul style="list-style-type: none"> • Receive call from affected official (ECDSD ICT Systems administrators /database administrators) • Register the incident with Helpdesk • Login into Veeam Backup and Replication Console • Open the restore wizard • Locate all the restore point • Select type of file to be restore (Application File or System File) • Perform the file restoration (Backup/Replication) • Inform the affected official on successful file restoration for them to test if missing or corrupt file is accessible. • Once official confirm all files are restored to original state • Change incident to resolve on the Helpdesk System • Notify Helpdesk to close call • Document and sign the restoration and file process as POE. <p>Or in case of damaged of corrupt Virtual Server</p> <ul style="list-style-type: none"> • Receive call from affected official or owner • Register the incident with Helpdesk • Login into Veeam Backup and Replication Console • Open the restore wizard • Locate all the restore point 			<p>Restored files View of restored files</p> <p>Server up and running View of the Server</p>	

STEP BY STEP GUIDE						
MONITORING OF DAILY BACKUP JOBS ON VEEAM						
Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
		<ul style="list-style-type: none"> Select VM type to be restore (VM to original Location or different location) Restore the affected VM (Backup/Replication) Inform the affected official on successful server restoration. Change incident to resolve on the Helpdesk System Notify Helpdesk to close call Document and sign server restoration procedure taken. <p>In the case where Backup and Replication server is inaccessible</p> <ul style="list-style-type: none"> Notify supervisor Log incident with Helpdesk Inform ICT DD/AD Datacentre Management of the failure ICT DD/AD Datacentre Management troubleshoot and remediate. Inform ICT Infrastructure of resolution. Test access If access is restored Notify helpdesk to close call. <p>Else in case of Network issues</p> <ul style="list-style-type: none"> Log a call with data line service provider Notify Supervisor Record the incident Service Provider attend to the call Receive feedback from service provider on resolution Close call with SITA 				

STEP BY STEP GUIDE						
MONITORING OF DAILY BACKUP JOBS ON VEEAM						
Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
6.	Request second line support from Veeam Support team	<p>If the error is not resolved</p> <ul style="list-style-type: none"> • Inform DD: ICT Infrastructure • Escalate the error to Level 400 Veeam Support team by e-mail/Telephonically • Veeam Support resolves error • Receive root cause report from Veeam support • Document resolution • Close call 	AD: ICT Infrastructure	1-3 days depending on the kind of error	<ul style="list-style-type: none"> • Resolved error • Incident Report 	
7.	Perform ongoing research on backup and replication and other solution	<ul style="list-style-type: none"> • Participate in backup and replication solution forums. • Compare solution results for their advantages and disadvantages. 	AD: ICT Infrastructure	3hr	<ul style="list-style-type: none"> • List of solutions that we can choose from 	
8.	Monitor solution license contract	<ul style="list-style-type: none"> • Open Backup (Veeam) Console. • Take in account the start and end of the licence. • Inform ICT Operations and Supply Chain three months before the new financial about the expiry of the licence for upgrade procurement arrangements by following Procurement Process. 	DD ICT Infrastructure	2hrs	<ul style="list-style-type: none"> • E-mail notification about the expiry of the solution • Report for solution expiry 	
9.	Participate in Backup and Replication software upgrades	<ul style="list-style-type: none"> • Participate in the software solution drafting specification. • Ensure that the upgrade installation or implementation is according to the specification. 	DD ICT Infrastructure	1 Day	<ul style="list-style-type: none"> • Project Charter • Testing Report • Project closure report 	

STEP BY STEP GUIDE						
MONITORING OF DAILY BACKUP JOBS ON VEEAM						
Nr	Task Name	Task Procedure	Responsibility	Time Frame	Supporting Documentation	Service Standard
10.	Ensure Monitoring of Backups schedules, Replication and testing	<ul style="list-style-type: none"> Record backup schedules. Test backup and restore procedures Verify test results (Database administrators/Systems Administrator/Datacentre administrators) Submit signed monthly backup testing report 	AD: ICT Infrastructure	1 Day	<ul style="list-style-type: none"> Monthly signed Backup schedules reports Testing report 	
11.	Evaluate and Review Backup process	<ul style="list-style-type: none"> Receive the backup report Evaluate backup process followed for the month Approve and sign the report Submit signed report to governance and compliance officer. File the approved report 	DD: ICT Infrastructure	1 Day	<ul style="list-style-type: none"> Signed backup report Approved backup report 	





PROCESS RISKS

Risk Name	Risk Description	Probability (H/M/L)	Impact (H/M/L)	Control Description	System / Manual
Unavailability of Level 400 Support	Expired licensing and OEM support maintenance not renewed at renewal intervals	H	H	Budget to be made available for license renewal at renewal intervals.	Manual
Unavailability of Skilled resource	Unable to resolve backup and DR replication error timeously as the ICT skill set is not at advance stage and staff are more reliant on the service provider or OEM support.	H	H	Capacitate at least 3 ICT staff as it will enable ICT to remediate errors as soon as it has been realised.	Manual

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

Document Name	Section Description or Document Description
Constitution of the Republic of South Africa (1996)	Constitution of the Republic of South Africa Section 32(1)(a) of the Constitution of the Republic of South Africa, 1996 provides that everyone has a right of access to any information held by the state and any information held by another person that is required for the exercise or protection of any rights.
The Promotion of Access to Information Act, 2000 (PAIA) (Act No. 2 of 2000)	The Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) (hereinafter referred to as "PAIA") is the national legislation which was enacted to give effect to the constitutional right of access to information. PAIA gives all South Africans the right to have access to records held by the state, government institutions and private bodies.
ISO 27001: (2005)	Information Security Management System ISO 27001:2005 (10) (4) states that Business Continuity Management Maintenance of essential business activities during adverse conditions, from coping with major disasters to minor, local issues Information Security Management System ISO 27001:2005 (6)(3) states that Communications and Operations Management: Examines correct management and secure operation of information processing facilities during day-to-day activities
Protection of Personal information Act (No 4 of 2013)	Section 19. (1) states that a responsible party must ensure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent - a) loss of, damage to or unauthorised destruction of personal information;
Minimum information Security Standard (MISS)	Minimum Information Security Standard (MISS) Chapter 4 (17) (17.1) The contingency plan of an institution must provide for the destruction, storage and/or moving of classified/sensitive documents in the event of an emergency in order to prevent the risk of being compromised.
Public Finance Management Act (PFMA)	Section 45(a) states that the officials of a Department must take effective and appropriate steps to prevent, within that official's area of responsibility, any unauthorised expenditure, irregular expenditure and fruitless and wasteful expenditure and any under collection of revenue due;

AUTHORISATIONS

Designation:	Name:	Comments:	Signature:	Date:
Recommended By: Director-	T.M. Vazi	The backup SOP will address all the aspects of server and data backup		03/02/2022
Recommended by: Acting CIO -	M.E.Gazi	Aligned with the new back up ICT policies		04/02/2022
Recommended by: DDG	N.Z.G Yokwana	Recommended.		09/02/2022
Approved by: HOD	M. Machemba	Approved		11/02/2022
Distribution and Use of SOP	All CIO Directors, All CIO Deputy Directors, All CIO Assistant Directors, All CIO Administration support staff, All CIO Personal Assistance			