



APPENDIX C-1(SERVICE LEVEL DESCRIPTIONS)/APPENDIX C-2 (KEY PERFORMANCE INDICATORS) BACK UP AS A SERVICE (“BaaS”)

Table of Contents

1. Introduction.....	3
2. Abbreviations.....	3
3. Definitions.....	4
4. Eskom DR Blueprint	5
5. Service Level Requirements Overview	5
6. Service Level Agreement Requirements.....	6
5.1. Front-End Server Backup	6
5.2. Endpoint Devices	6
7. Service Level Requirements KPIs – Server Backup/Restore	7
8. Monthly Service Level Requirements KPIs – End Points	8

1. Introduction

This Service Level Agreement defines the service performance requirements for Backup as a Service (BaaS) to Eskom, including managed backup, replication, recovery, restore validation, monitoring, and reporting across Eskom's on-premises, cloud, and hybrid environments.

BaaS supports Eskom's data protection, disaster recovery, and IT business continuity requirements by enabling protected data to be recovered in accordance with agreed service levels, retention requirements, CMDB classifications, application criticality, Recovery Time Objectives (RTOs), and Recovery Point Objectives (RPOs). Backup does not replace disaster recovery; however, it is a critical recovery capability within Eskom's broader resilience framework.

2. Abbreviations

Abbreviation	Explanation
BaaS	Backup as a Service
CI	Configuration Item
CMDB	Configuration Management Database
CSI	Continuous Service Improvement
DBA	Database Administrator
DR	Disaster Recovery
EUC	End-User Computing
IT	Information Technology
KPI	Key Performance Indicator
LAN	Local Area Network
MTTR	Mean Time to Resolve
P1 / P2	Priority 1 / Priority 2
RCA	Root Cause Analysis
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Service Level Agreement
SQL	Structured Query Language
TBA	To Be Advised

3. Definitions

Term	Definition and Explanation
Application Criticality	The classification of an application or system based on its importance to Eskom's business operations and recovery requirements.
Backup Success Rate	The percentage of valid scheduled backup jobs completed successfully during the applicable Measurement Period, calculated after excluding approved exclusions and Excused Events in accordance with Schedule C (Performance Standard).
Backup Testing	The periodic testing of selected backups to confirm that data can be restored successfully.
Configuration Item	An item recorded in the CMDB that is required to deliver or support IT services, including servers, systems, applications or endpoint devices.
Coverage Report	A report that confirms the systems, applications or endpoint devices covered by the backup service and compares the coverage against the CMDB where applicable.
Defective Service Level	The performance threshold specified for a Service Level below which the applicable Performance Level Multiplier and contractual remedies associated with defective performance may apply.
Endpoint Device	An Eskom-issued user device that is included in the endpoint backup service, where applicable.
Material Default Service Level	The performance threshold specified for a Service Level below which the applicable Performance Level Multiplier and contractual remedies associated with material default performance may apply.
Measurement Period	The period specified for measuring performance against a Service Level or KPI, as set out in Appendix C-1 and interpreted in accordance with Schedule C (Service Performance).
Offsite Replication	The copying of backup data to an alternate or designated recovery location for resilience, disaster recovery or long-term retention purposes.
Recovery Point Objective	The maximum acceptable amount of data loss measured in time, as defined for the relevant system, application or service.
Recovery Time Objective (RTO)	The maximum acceptable time within which a system, application, service or data set must be restored following an incident or disruption.
Replication Success	The successful copying of completed backup data to the designated offsite or disaster recovery location.
Restore Success	Successful completion of a valid operational restore request, with the restored data or system made available in a usable state.
Restore Validation	Controlled testing performed to verify the integrity, recoverability and usability of selected backup data without necessarily responding to an operational restore request.
Service Category	The area of service being measured, such as backup, restore, replication, reporting or service management.
Service Level Agreement	The agreed measurable service performance requirements applicable to the BaaS Services, including the applicable measurements, targets, Measurement Periods and reporting obligations.
Service Level ID	A unique identifier for each KPI or service level requirement.
Target Service Level	The required level of Service Level Performance that the Supplier must meet or exceed during the applicable Measurement Period.
Weighting Percentage	The percentage weighting assigned to a KPI for service performance assessment or service credit calculation, where applicable.

4. Eskom DR Blueprint

System importance to Eskom	Safety and Revenue Critical	Mission Critical	Business Critical	Normal to non-essential
Eskom Definition	Failure of system functions may result in injury death or major revenue loss and reputational damage	Vital to the functioning of an Organisation and the accomplishment of its mission	Without which the Business can still run for a predefined period	
Time Loss (RTO)	Continuous Processing	4 - 8 hours	<48 hours	>72 Hours
Data Loss (RPO)	=0 (No Loss)	=0 (No Loss)	<24 Hours after Data Loss incident	<24 Hours after Data Loss incident
DR Blueprint Recovery	Application specific design: 1. Log Shipping 2. RAC Storage Replication	Asynchronous SAN-replication of boot and appl. disks. Recovery boot DR server from SAN	Configuration Man. Processes on all servers to ensure warm server in place	Restore from Backup
Supporting Infrastructure	SAN Replication, Reliable IDC+ Geo-stretch clusters	SAN Replication, Reliable IDC, VMWare Live Recovery	Reliable IDC	Reliable IDC
Timeliness – Data Backup	99.50% of all backups complete successfully within the identified backup window Note - failed consecutive incremental backups or a failed complete backup should generate a Priority 2 Incident			
Timeliness – Data Restore	95.0% within 4 hours of media being onsite and 100% successful restore			

5. Service Level Requirements Overview

For each service item described in the Scope of Work, Eskom has defined the following requirements in the KPI table below:

- A Target Service Level;
- A Defective Level;
- A Material Default Level;
- A Measurement Period applicable to the relevant Service Level.

Service items will be monitored during their respective Measurement Periods, as specified in Schedule C (Performance Standards).

6. Service Level Agreement Requirements

5.1. Front-End Server Backup

Eskom defines three service tiers based on the business criticality of the relevant environment. The SLA metrics below apply to all tiers, with performance measured and reported in accordance with the specified frequency and target levels.

Measurement	Frequency	Target
Backup Success Rate	Daily	≥ 95% of scheduled backup jobs must complete successfully
Backup Replication	Daily	100% of successfully completed backups must be replicated to the designated DR site with 8 hours
Restore Success	On-demand or DR testing	100% of successfully backed-up systems selected for restore validation must be restorable
Tape Restore SLA	As required	Backup tapes must be delivered to the impacted site within 4 hours of request, where operationally feasible and commercially agreed
Backup Testing	Quarterly (every 3 to 4 months)	100% of tested backups must pass restore validation

These SLA metrics support data availability, operational resilience, and compliance with Eskom's business continuity and disaster recovery objectives.

Eskom system classifications must be considered when finalising the solution design and confirming the applicable backup, replication, and restore requirements.

5.2. Endpoint Devices

The following SLA metrics apply to endpoint backup services and are intended to ensure consistent data protection and recovery capability for Eskom-issued user devices.

Measurement	Frequency	Target
Backup Success Rate	Weekly	≥ 95% of scheduled endpoint backups must complete successfully
Restore Success	On request	All successfully backed-up endpoint devices selected for restore validation must be restorable
Backup Testing	Quarterly (every 3 to 4 months)	100% of tested endpoint backups must pass restore validation

These SLAs are designed to ensure that user data is reliably protected and recoverable, while supporting Eskom's wider compliance and business continuity objectives.

7. Service Level Requirements KPIs – Server Backup/Restore

KPI#	KPI	KPI Description	Std	Adv	Prem	Weight	Server
BaaS_01	Backup Success Rate by Eskom Application Classification	Percentage of scheduled backup clients per Backup window completed successfully, measured per system daily aggregated over a 30-day period.	Target			20%	All backups complete successfully within the identified backup window as per the CMDB and measured per system classification
			≥ 92%	≥ 95%	≥ 98%		
BaaS_02	Restore Success Rate	Valid restore requests from the business, application owner, or authorised service owner must be fulfilled using available backup data within the agreed retention period.	100% of valid restore requests and selected point-in-time restore tests must be completed successfully within the agreed retention period.			35%	Valid restore requests must be fulfilled for confirmed recovery points using available backup data within the agreed retention period. Recovery points must be confirmed by the application teams and DBAs before restore execution.
BaaS_03	Consecutive Backup Failures	Number of unresolved consecutive backup failures per server within a Backup window aggregated over 30-days.	8%	5%	2%	15%	A consecutive failure occurs where a backup fails for two consecutive days and remains unresolved. Note - failed consecutive backups or a failed complete backup should generate a Priority 2 Incident
BaaS_04	Replication Success Rate	Percentage of successfully completed backups replicated to the designated DR or offsite location, measured daily and reported monthly.	100% of daily, weekly, and monthly backup copies must be replicated to the agreed DR or offsite retention location.			10%	A replication report must be generated to reflect daily, weekly, and monthly replication and deduplication status.
BaaS_05	Timely Backup Report Upload Rate	Daily, weekly, and monthly reports, based on the agreed reporting list provided to the Supplier.	Maximum tolerance of 5% for reports not uploaded to the portal within a 7-day period.			5%	Reports should be updated daily on the portal, and all issues and remedial plans should be highlighted in the supporting documents
BaaS_06	Backup Coverage Report	100% of all CIs marked for backup must be included in the coverage report.	Quarterly coverage reports must achieve at least 98% accuracy when reconciled against the CMDB.			10%	The coverage report must be produced quarterly.
BaaS_07	Tape Backup	Ensure reliable long-term data protection through successful tape backup operations and recoverable backup data.	Delivery of Tape media to the required location within 8 hours of the request			15%	The tape solution is an alternative to disk-based Backup where there is no option to replicate Backup Data

8. Monthly Service Level Requirements KPIs – End Points

KPI#	KPI	KPI Description	Target		
BaaS-101	Endpoint Backup Success Rate	Ensure successful backup of endpoint devices (laptops, desktops, and mobile devices where applicable) to protect business-critical user data.	98% of the devices on the Eskom LAN for the month in review		≥ 98%
					Meets SLA
					95% - 97.99%
					Service Improvement Required
					< 95%
					SLA Breach
BaaS-102	Restore Request Fulfilment	Restore endpoint data within agreed service levels.	Standard User	Within 4 Hour	
BaaS-103	Endpoint Recovery Success Rate	Ensure endpoint data can be successfully recovered when required.	Recovery Success rate = 99%		
BaaS-104	Backup Agent Health Compliance	Maintain healthy and operational backup agents on endpoint devices	Agent Health Compliance (%) = 98%		
BaaS-105	Backup Policy Compliance	Ensure endpoint devices adhere to approved backup policies	100% Policy Compliance		Measurements: - Scheduled backup frequency - Retention policy compliance - Encryption compliance - Backup storage compliance
BaaS-106	Endpoint Data Encryption Compliance	Protect backed-up endpoint data against unauthorized access.	100% of endpoint backups encrypted at rest and in transit.		
BaaS-107	Endpoint Protection Coverage	Ensure all authorized endpoint devices are protected by the backup solution	100% of the devices on the Eskom LAN for the month in review		