Infrastructure Support managed Service - STATEMENT OF WORK

CORP 5527 - AUGUST 2020

Table of Contents

Page

[1 Infrastructure Support Managed Service Overview and Objectives 2](#_Toc79666376)

[1.1 Infrastructure Support Managed Service Overview 2](#_Toc79666377)

[1.2 Environments in Scope 2](#_Toc79666378)

[1.3 Services in Scope 3](#_Toc79666379)

[1.4 Service Objectives 4](#_Toc79666380)

[1.5 Personnel 4](#_Toc79666381)

[1.6 Policies, Procedures and Standards 4](#_Toc79666382)

[1.7 Agreements and Licences 4](#_Toc79666383)

[2 Roles and Responsibilities 5](#_Toc79666384)

[2.1 General Roles and Responsibilities 5](#_Toc79666385)

[2.2 Managed Services 8](#_Toc79666386)

[2.3 Server Maintenance and Refresh Services 11](#_Toc79666387)

[2.4 Storage and Data Management Services 14](#_Toc79666388)

[2.5 Network Management 18](#_Toc79666389)

[2.6 Incident and Problem Management 18](#_Toc79666390)

[2.7 Information Security Management Services 20](#_Toc79666391)

[2.8 Configuration Tracking 23](#_Toc79666392)

[2.9 Capacity and Performance Management 24](#_Toc79666393)

[2.10 Customer Satisfaction 24](#_Toc79666394)

[2.11 Disaster Recovery Services 25](#_Toc79666395)

[3 Inclusions 25](#_Toc79666396)

[4 Exclusions 26](#_Toc79666397)

[5 Appendices 27](#_Toc79666398)

# Infrastructure Support Managed Service Overview and Objectives

## Infrastructure Support Managed Service Overview

This Statement of Work SOW sets forth the roles and responsibilities between Eskom and the Supplier for an infrastructure support managed service offering. Eskom requires the Tenderer to provide locally based server, storage and backup support services through a managed service offering i.e. Supplier must have a local presence and supply support services on Eskom owned infrastructure hosted at various Eskom sites. These services will be driven by policies, processes and procedures in support of our day-to-day operations, application lifecycle management and business processes. Eskom requires a managed service offering that delivers the following services:

* Server Provisioning and Support Services (includes hardware and software and covers Virtualisation, Hypervisors and Operating Systems);
* Data Storage Provisioning and Support Services (includes hardware and software);
* Backup Provisioning and Support Services (includes hardware and software);
* Incident and Problem Management
* OEM vendor management on behalf of Eskom
* Information Security Services
* Disaster Recovery (DR)
* Supporting systems software
  + Virtualisation/Hypervisor software
  + Operating Systems (OS)
  + Operating Systems utilities

The infrastructure environments host Eskom’s business applications, file/print services and other specific infrastructure-related functions (for example, Client single sign-on application). The Supplier may deploy additional systems (need to comply with Eskom policies & standards) to support the computing environment and to provide Eskom’s infrastructure technical support.

## Environments in Scope

The environments in the scope of this RFP are defined as follows:

1. Current Eskom owned infrastructure environment: Eskom’s currently allocated and utilized computing resources On-Premise, including any associated disaster recovery environments, as per Eskom’s specification. This includes servers, storage and backups and encompasses both physical and virtualized environments. The Supplier must provide locally based server, storage and backup support services for these environments. These environments are described Appendix A

The above-mentioned environments are hosted within the borders of South Africa and conform to Eskom’s technology standards as defined in Table 1: Infrastructure Technology Standards

**Table 1: Infrastructure Technology Standards**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CPU Architecture** | **Operating Systems** | **Virtualization** | **Storage** | **Backups** |
| X86  Non X86(RISC) | Windows Server  LINUX   * + SUSE   + Red Hat   + Oracle-Linux   UNIX   * + AIX   + Solaris   + HP-UX | VMware  Oracle Virtual Machine Manager  PowerVM  HyperV | Tier 0 (All Flash)  Tier 1 (Enterprise)  Tier 2 (Auto Tiering)  Tier 3 (Nearline) | Netbackup  Spectrum Protect |

## Services in Scope

The following services are required to be provided by the Supplier:

* Provisioning of IT Infrastructure to cater for Eskom user demands
* Infrastructure management, support and maintenance of the environments in scope
* Backup and storage services
* Assist with troubleshooting of Network services as well as new installation requirements
* Virtual server and Operating System provisioning and support. (Including utilities and schedulers)
* Incident and Problem Management
* Disaster Recovery services
* Information Security services
* Monitoring
* Reporting

## Service Objectives

The following are the key high-level service objectives Eskom expects to achieve through outsourced managed services in this SOW:

* Meet Eskom’s business needs for highly available, reliable, scalable and secure services.
* Maintain compliance with industry standards and government regulations (eg. ITIL, ISO27000, and Six Sigma).
* Acquire services with availability guarantees backed by service levels (SLs) and associated penalties in the form of fee reductions with full earn-back opportunities.
* Acquire services that can leverage operational scale and best practices to achieve optimum commercial price performance.
* Acquire ongoing feedback mechanisms to ensure performance meets expectations.
* Support services may be required 24x7 as needed i.e. some support activities are required to be provided outside normal business hours to prevent disruption to Eskom business. This should be provided at no additional cost.

## Personnel

Unless otherwise specified and agreed to by the Eskom and Supplier, the Supplier will be responsible for providing appropriately skilled staffing to meet all managed services roles and responsibilities with the relevant service levels set forth in this SOW. The Supplier should also be able to supply adequately skilled resources for future requirements e.g. when new technologies are introduced in the Eskom landscape.

## Policies, Procedures and Standards

* The Supplier needs to adhere to Eskom’s policies, procedures and standards.
* The Supplier needs to adhere to the Eskom Architecture Standards.
* The Supplier needs to adhere to the Eskom Information Security Policy.
* The Supplier must comply with South Africa Information Security Acts
* Electronic Communications and Transactions Act 2002;
* Regulation of Interception of Communications and Provision of Communication-Related; Information Act 2002;
* Protection of Personal Information Act 2015;
* National Cybersecurity Policy Framework 2012; and
* Cybercrimes and Cybersecurity Bills.
* Any relevant Eskom policies and procedures

## Agreements and Licences

* Licenses will be supplied by Eskom for the Eskom owned software.
* Hardware maintenance and support will be the responsibility of the Eskom for all Eskom owned infrastructure, for the duration of the contract. For all operational activities the supplier will be required to interface with the maintenance supplier/OEM, on behalf of Eskom e.g. break-fix activities.
* Monitoring toolset/s to be supplied by the Supplier.

# Roles and Responsibilities

The services should cover all Eskom’s generic computational needs to support its commercial and custom software/applications. The Supplier is responsible for delivering all services defined in this SOW under the following nomenclature:

*In this SOW, we have defined the services required and used a RASCI chart approach to assign a roles and responsibilities matrices.*

RASCI stands for:

R = responsible

A = accountable

S = supporting

C = consulted

I = informed

Eskom requires more than just the support activities performed by the Supplier. These activities, include but are not limited to planning and analysis, service-level monitoring and reporting, and performance management, which should be referenced from the Cross-Functional Cloud Services SOW (Appendix C). The Supplier needs to supply their own monitoring toolset. The monitoring toolset needs to seamlessly integrate into the existing Cross-Functional Monitoring and Service desk function.

## General Roles and Responsibilities

The Supplier is expected to perform the following general responsibilities:

* Server (including VM, Hypervisor and OS installation and setup), Storage and Backup provisioning activities (including installations and setup)
* Server (including VM, Hypervisor and OS), Storage and Backup support and operations activities
* Server, Storage and Backup change management activities
* Server, Storage and Backup hardware maintenance operational activities

The following tables identify general roles and responsibilities associated with this SOW. The letter “R" is placed in the column under the Party that will be responsible for performing the task. Supplier responsibilities are indicated in the column labelled "Supplier."

Table 2: General Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **General Role and Responsibilities** | **Supplier** | **Eskom** |
| 1. Manage and operate Eskom’s current servers, storage and backup infrastructure within the scope of this managed service. | R,A | I,C |
| 1. Provide preventative measures for proactive monitoring and self-healing capabilities to limit outages that impact service delivery. | R,A | I,C,S |
| 1. For Security and Data Protection purposes, the distance between the Production and DR/Replication Data Centres must be a minimum of 20 km apart. | I | R, A |
| 1. Current Infrastructure landscape: Eskom to provide and support the related environmental elements for hosting (e.g., HVAC, dual-redundant UPS, power, cable plant, fire detection and suppression systems, temperature and humidity controls, and controlled physical access with 24/7 manned security). | I,C | R,A |
| 1. Provide technical support for all hardware/equipment of the infrastructure. | R, A | I |
| 1. Provide technical support for all relevant software e.g., operating systems, utilities, storage and backup software etc. | R, A | I |
| 1. Current Infrastructure landscape: Eskom to provide and support Networks i.e. LAN and WAN connections and related operations (e.g., procure, design, build, systems monitoring, incident diagnostics, troubleshooting, resolution and escalation, security management, and capacity planning/analysis), as required, to meet Eskom's computing requirements. | I | R, A |
| 1. Comply with Eskom policies and standards and regulations, including information systems, change management, personnel, architecture standards, physical and technical security. | R,A | I,C |
| 1. Security controls must be implemented and maintained to prevent leakage of the Eskom's data. | R,A | I,C |
| 1. Protect Eskom's data and systems from unauthorized access always. | R,A | I,C |
| 1. Define policies and procedures regarding the support\service requests that are in line with Eskom’s support\service desk capabilities. | R,A | I,C |
| 1. Create, maintain and provide all appropriate project plans, project time and cost estimates, technical specifications, management documentation and management reporting in a form/format that is acceptable to Eskom. | R, A | C, S |
| 1. Provide a service\support request capability that integrates into Eskom’s enterprise service desk capabilities. | R,A | I,C |
| 1. Allow Eskom to log, track and trace support\service requests with the Supplier via Eskom’s service desk capabilities. | R,A | I,C,S |
| 1. Provide the capability to seamlessly integrate into Eskom’s Cloud Management Platform (CMP). (CMP is IBM CloudForms) | R, A | C, S |
| 1. Supplier to provide relevant infrastructure monitoring toolsets. All Supplier monitoring toolsets must seamlessly integrate into Eskom’s MARC and SIEM solutions. This will adhere to all Eskom security policies and architectural standards | R, A | C, S |

## Managed Services

### Operations, Administration and Management

Operations and administration services are the activities associated with the day‑to‑day management of the environment. They provide and support a stable infrastructure and effectively and efficiently perform operational and processing procedures to ensure services meet SLA targets. Table 3: Operations, Administration and Management Roles and Responsibilities identifies the operations and administration roles and responsibilities that the Supplier and Eskom will perform.

Table 3: Operations, Administration and Management Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| Server Operations, Administration and Management Roles and Responsibilities | Supplier | Eskom |
| 1. Define monitoring requirements and policies. | C, I | R, A |
| 1. Develop monitoring procedures that meet requirements and adhere to defined policies, and document in the standards and procedures manual. | R, A | I |
| 1. Review and approve monitoring procedures. | C, I | R, A |
| 1. Provide proactive and scheduled console monitoring of infrastructure and systems (e.g., hardware, OS, network, batch schedule, interfaces etc.), respond to messages and take corrective action as required. Monitoring should cover performance, availability etc. | R, A | I |
| 1. Develop and maintain standard automated scripts to perform monitoring on systems software. | R, A | C, S |
| 1. Monitoring toolset should provide seamless integration into the Monitoring and Response Centre (MARC) and Service Desk call logging facility for the logging of auto-generated tickets. | R, A | C, S |
| 1. Provide various monthly availability and performance reports for Eskom, such to be defined and revised periodically (e.g. executive summary, departmental, drill down capability, ad hoc). | R, A | I |
| 1. Identify and report problems, including system, file and disk problems. | R, A | I |
| 1. Provide troubleshooting, repair and escalation of problems in the computing environment. | R, A | I |
| 1. Provide preventative measures for proactive monitoring and self-healing capabilities to limit outages that impact service delivery. | R, A | I |
| 1. Assist in resolving application problems stemming from the Operating System or other Supplier related services and escalate, as required. | R, A | C,S |
| **System Administration and Management Roles and Responsibilities** | **Supplier** | **Eskom** |
| 1. Define system administration requirements and policies. | C | R, A |
| 1. Develop procedures for performing system administration that meet requirements and adhere to defined policies, and document in the standards and procedures manual. | R, A | I |
| 1. Review and approve systems administration procedures. | C, I | R, A |
| 1. Perform system or component configuration changes necessary to support computing services in conformance with change management requirements. | R, A | I,C |
| 1. Provide usage statistics reports that will be used to support chargeback and other reporting requirements. | R, A | I,C |
| 1. Prepare various monthly availability and performance reports for Eskom, such to be defined and revised periodically (e.g. executive summary, departmental, drill down capability, ad hoc) | R, A | I |
| 1. Provide data, information and assistance required for demand planning by Eskom on a monthly basis and ad-hoc requests when requested. | R, A | I |
| 1. Generate monthly capacity reports indicating usage and trends. | R, A | I |
| 1. Provide data, information and assistance in developing a Disaster Recovery (“DR”) Plan and assist in disaster recovery activities during an actual disaster and DR plan testing as per Eskom’s DR policies and procedures (currently required twice a year per plan). | R, A | I |
| 1. Provide cabling requirements for connection of Eskom’s Servers to Data Centre Network and Storage and Backup devices. | R, A | C, S |
| 1. Make technical audit skills available as and when requested by Eskom in respect of the auditing of security configuration, designs, alterations, planning, etc. | R, A | I |
| 1. Provision a new virtual server with standard configuration (preferably from a template) | R, A | I |
| 1. Make future copies of such virtual servers available to Eskom free of charge (This should be stated as such in the standard pricing for Support Services) | R, A | I |
| 1. Provide assistance to the End-User Computing (EUC) Supplier for the installation of thin client software | R, A | I |
| 1. Perform all work necessary to enable Eskom’s servers to connect to external storage | R, A | C |
| 1. Provide support/assistance for complex application troubleshooting | R, A | I |
| 1. Deploy and manage server related patches in alignment with the Eskom Policies (N-1). | R, A | I |
| 1. For clustered systems - Configure and maintain clusters and balance/sync cluster services after cluster (OS and hypervisor) node failure. | R, A |  |
| 1. Manage security software/agents deployed to Eskom’s Servers. | R,A | C,S |
| 1. Operational support of antimalware agent and outbreak management. Ensure that Eskom’s Servers are virus and malware free. | R,A | C,S |
| 1. Ensure compliance with the Eskom Information Security Policy, relevant Eskom Policies, as well as such technical standards, guidelines and procedures as Eskom may prescribe from time to time. | R, A | I |
| 1. Harden Eskom Servers in line with Eskom’s technical security standards. Support the Eskom exceptions process where technical security controls cannot be applied. | R, A | I |
| 1. Proactive reporting of compliance and risk as directed by Eskom. | R,A | I |
| 1. Provide information related to the creation and administration of user accounts and user groups (including permissions, environment and rights) | R, A | I |
| 1. Timeously inform Eskom when the Supplier becomes aware of risks or vulnerabilities as per Eskom’s risk management process. | R, A | I |
| 1. The remediation of risks and vulnerabilities as agreed with Eskom within the scope of Server Support Services. Eskom retains the responsibility for approving the remediation of all vulnerabilities and risks raised by the Supplier prior to any work being carried out. | R, A | I |
| 1. Timeously report security breaches, compromises or incidents, or suspected security incidents to the Eskom Information Security Manager, and support investigation and retention of evidence if required. | R, A | I |

## Server Maintenance and Refresh Services

Maintenance and Refresh services are the preventative maintenance activities performed to ensure that service is stable and will not fail. This service includes hardware and software maintenance, firmware, OS, hypervisor etc. It also includes activities needed to ensure that the infrastructure is configured in accordance with Eskom’s Policies and directions.

The Supplier will ensure installation of required monitoring applications, anti-malware, security agents and non-OS related software.

Table 4: Maintenance and Refresh Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Server Maintenance and Refresh Roles and Responsibilities (Part1)** | **Supplier** | **Eskom** |
| 1. Test and apply OS patches (both security and critical patches) and firmware updates according to Eskom Policies. | R, A | C,S |
| 1. Deploy and maintain latest anti-malware and all relevant security software agents in accordance with the Eskom Policies. Support outbreak management and ensure that the servers are virus and/or malware free. | R, A | I |
| 1. Support and maintain all OS-related software components. | R, A | I |
| 1. Implement Eskom Policies, and specifically Eskom’s security policies and technical security standards, and ensure that Eskom’s Servers remain compliant. Supplier shall report any instances of non-compliance to the Eskom Information Security Manager. | R, A | I |
| 1. Provide accurate documentation of the processes and procedures as required by Eskom (e.g. system configuration, antimalware procedures) | R, A | I |
| 1. Maintain OS and hypervisor logs files; also ensure that these files are regularly backed up and cleaned out in order to ensure that sufficient space is available for subsequent log files to be written to the disk | R, A | I |
| 1. Co-ordinate and facilitate the replacement of components that are showing early failure warnings | R, A | I |
| 1. Advise Eskom of upcoming policy violations (e.g. Licensing Age). Ensure this is done timeously. | R, A | I |
| 1. Ensure correct migration to new platform during a technology refresh when required (e.g. migration activities to move EOL hardware to new hardware platforms, physical to virtual, traditional IT systems to cloud based solutions etc.) | R, A | C |
| 1. Assess and modify system configuration files, validate integrity of system configuration files | R, A | C |
| 1. Adopt a template based provisioning model. Create and maintain virtual machine templates. | R, A | C |
| 1. Repair defective file systems | R, A | I |
| 1. On-demand restart / reboot a server | R, A | I |
| **Server Maintenance and Refresh Roles and Responsibilities (Part 2) - Operational Activities needed to support Eskom’s ongoing development and project activities** | **Supplier** | **Eskom** |
| 1. Modify network settings and ports related to the server infrastructure | R, A | C |
| 1. Manage file systems including creating, maintaining and deleting volumes and directory structures | R, A | C |
| 1. Manually move a virtual server to another host mainly for performance reasons (but not limited thereto) | R, A | I |
| 1. Perform all server, storage and backup work necessary to enable restore of backup images when requested. | R, A | C |
| 1. Create file systems when it requires disc resource to be assigned | R, A | I |
| 1. Add cores and RAM memory to a virtual server | R, A | I |
| 1. Perform memory upgrades for a physical server | R, A | I |
| 1. Move physical servers inside a Data Centre facility / server room | R, A | I |
| 1. Move physical servers between Data Centres / server rooms. Migrate Eskom Server(s) from physical to virtual, virtual to virtual, and virtual to physical environments | R, A | I |
| 1. Upgrade server OS version for a Server (excluding application level regression testing which will be executed by the Application Support Team) | R, A | I |
| 1. Install, configure or modify a cluster configuration (e.g. create a new cluster service) | R, A | I |
| 1. Add and remove disk space | R, A | I |
| 1. Decommission and sanitise a virtual server in accordance with the Eskom Information Security Policy | R, A | I |
| 1. Decommission and sanitise a physical server in accordance with the Eskom Information Security Policy. | R, A | I |
| 1. Provide assistance to Eskom Supplier/s during Change activities, e.g. including but not limited to, Network upgrades, Data Centre Power upgrades etc. | R, A | C |
| 1. If project management services are required for provisioning or change activities, the change and provisioning activities will be included in the standard pricing for support services. However, if required in Eskom’s discretion, the project management service will be negotiated and billable on a time and materials basis at Supplier’s standard rates. | R, A | C |

## Storage and Data Management Services

Storage and data management services are the activities associated with the provisioning and day‑to‑day management of the installed storage and data environment. These include, for example, direct access storage devices (DASD), redundant array of independent disks (RAID), storage area network (SAN) including the associated storage networking infrastructure eg. SAN switches, network-attached storage (NAS), and tape and optical, providing a stable support infrastructure and effectively and efficiently performing procedures to ensure services meet SLR targets and requirements.

This service also includes the activities associated with the provisioning and day‑to‑day management of the installed backup environment. Backup services are aimed at addressing any issue or requirement related to data loss, data corruption or Disaster Recovery.

With respect to the backups of the Eskom SAP environment which is backed up using Spectrum Protect, Eskom may require this service from the Supplier. If this service is required, The Supplier is required to supply two options. Option one is to provide a managed service backup support for the SAP Spectrum environment and option two is to take over the existing hardware, supply the Spectrum Protect software and provide the backup support service i.e. take over the existing SAP Spectrum environment and provide it back as a service. The purchased hardware will also need to be refreshed once it reaches end of life.

Table 5 identifies the storage and data management roles and responsibilities that the Supplier and the Eskom will perform.

Table 5: Storage and Data Management Services Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| Storage and Data Management - Roles and Responsibilities | Supplier | Eskom |
| 1. Define Supplier standard storage and data management procedures. | R, A | C |
| 1. Develop storage and data management procedures that meet Eskom requirements and adhere to Eskom policies, and document and maintain in the standards and procedures manual. | R, A | I |
| 1. Review, provide additional procedures as required, and approve storage and data management procedures. | I | R, A |
| 1. Provide data storage services (e.g., Disk installation and configuration, Zoning, Host presentation in SVC, LUN creation, storage replication, RAID array, SAN, NAS, tape and optical). Manage break-fix resolution. | R, A | I |
| 1. Assist in incident and problem resolution for cross functional support matters. | R, A | C,S |
| 1. Perform storage monitoring, reporting (performance, availability, capacity planning), maintenance, troubleshooting and resolution. | R, A | I |
| 1. Monitor and control storage performance according to technical specifications and conduct performance tuning, as required. | R, A | I |
| 1. Maintain and improve storage resource efficiency. | R, A | I |
| 1. Maintain dataset placement and manage data catalogs. | R, A | I |
| **Backups - Roles and Responsibilities** | **Supplier** | **Eskom** |
| 1. Develop backup procedures that meet Eskom requirements and adhere to Eskom policies. | R, A | C |
| 1. Development of the SLP (Storage Lifecycle Policy) | R, A | C |
| 1. Review and approve backup policies and procedures. | C, S | R, A |
| 1. Provision and configure backup systems and backup clients for the server infrastructure. | R,A | I |
| 1. Provide backup scheduling, job execution, monitoring, reporting (including capacity planning), maintenance, troubleshooting and resolution, restores and backup replication, taking into account infrastructure and system interdependencies. Manage break-fix resolution. | R, A | I |
| 1. Management and active monitoring of backup schedules | R, A | C |
| 1. Monitoring and Reporting on Backup Success Rate | R, A | C |
| 1. Replicate and Restore of Backups at Target or DR site (TBA) | R, A | C |
| 1. Assist Eskom by providing required information for Audit purposes | R, A | I |
| 1. Migration of Backup Data from a Cloud Service Provider or other Service Providers, if required | R, A | C, S |
| 1. Log & Track, and coordinate calls for failures (break-fix) with vendors. | R, A | I |
| 1. Perform periodic backup and restore testing including during DR tests. | R, A | I |
| 1. Provide input processing for activities such as loading third-party media (e.g., tape) and receipt and/or transmission of batch files. | R, A | I |
| 1. Facilitate and manage consumables such as tape and disks in support of the backup requirements. Coordinate acquisition of additional materials as needed. | R, A | C, S |
| **Media Operations Roles and Responsibilities** | **Supplier** | **Eskom** |
| 1. Define Supplier-standard media operations procedures | R, A | C |
| 1. Develop, document and maintain in the Standards and Procedures Manual, media operations Supplier procedures that meet Eskom requirements and adhere to Eskom policies | R, A | C, S |
| 1. Review, provide additional procedures as required and approve media processing procedures | I | R, A |
| 1. Supply and Maintain a media library and media management system | R, A | I |
| 1. Manage the media inventory to ensure that adequate media resources are available and coordinate acquisition of additional media as needed | R, A | I |
| 1. Manage input media availability to meet processing SLR | R, A | I |
| 1. Load and manage third-party media | R, A | I |
| 1. Provide secure off-site storage for designated media and transport media to an Eskom approved off-site location as required | R, A | C, S |
| 1. Perform periodic audits to ensure proper cataloging of media | R, A | I |

## Network Management

The infrastructure in scope is hosted in Eskom facilities. All Network management services for the WAN and Datacentre LAN will be provided by the Eskom Network team.

Network management will cover the following services:

* Network troubleshooting for infrastructure supported by the Supplier.
* Network needs/requirements design for all new as well as existing infrastructure supported by the Supplier.

With respect to connectivity between the Supplier and the Eskom Network, all network connections into the Eskom Network will be established via a vendor neutral side. Eskom will extend its network to the vendor neutral site and connectivity from the Supplier to the vendor neutral site must be highly available and provided and managed by the Supplier. Connectivity from the vendor neutral site to Eskom will be highly available and provided and managed by Eskom.

## Incident and Problem Management

Incident and Problem Management service includes all the activities needed to actively resolve Incidents and to proactively close identified Problems.

For the Incident and Problem Management Roles and Responsibilities from the table above, Eskom follows ITIL Incident types and defines four priority levels of Incidents, depending on the level of severity: Priority 1, Priority 2, Priority 3 and Priority 4 (“Eskom Incident Types”), as set out in the Table below

Table 7: Eskom Incident Types

|  |  |  |
| --- | --- | --- |
| **ITIL Incident types** | **Eskom Incident types** | **Description (examples)** |
| **Critical** | **Priority 1** | Incident that causes unavailability of services running on Servers [On an Advanced or Premium support level].Examples:   * Production system not available. * Data corruption detected. |
| **Major** | **Priority 2** | Incident that causes deterioration of services running on Servers. Examples:   * Servers performance degraded (system not performing at acceptable levels), performance KPIs are below Defective Level. * Incidents with high risk of reoccurrence. * Incidents with high-risk of escalating to a Priority 1. |
| **Minor** | **Priority 3** | Incident with no impact on Server availability. Examples:   * One element of a cluster is not available but cluster is still operational Violation of Eskom’s Information Security Policy. * Eskom’s Servers are over-utilised (utilisation above a predefined maximum utilisation) (maximum utilisation to be agreed). * Eskom’s Servers are under-utilised (utilisation below a predefined minimum utilisation) (minimum utilisation to be agreed). |
| **Priority 4** | Non-urgent Incidents where a work around is available and Eskom has agreed to low priority classification. |

Table 8: Incident and Problem Management Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Incident and Problem Management Roles and Responsibilities** | **Supplier** | **Eskom** |
| 1. Provide Incident determination, resolution and reporting. | R, A | I |
| 1. Conduct root-cause analysis of outages, propose mitigation measures and provide Resolution details as per Eskom’s Policies (currently required for high severity Incidents (P1 as well as P2) on critical systems). This may also be requested on an ad hoc basis for other Incidents where Eskom deems it to be necessary. | R, A | I |
| 1. Assist in Resolution of cross functional problems and participate in problem management task teams (following ITIL problem management framework). | R, A | I |
| 1. Actively participate in Incident and Problem management for Server, Storage and Backup related problems. | R, A | I |
| 1. Troubleshoot infrastructure issues (including network, performance and security issues). | R, A | I |
| 1. The objective of the troubleshooting above is to identify if the issue is an application level issue, an infrastructure issue or an issue in an external service (e.g. LAN, WAN etc.) | R, A | I |
| 1. There are three possible outcomes of the troubleshooting activity:    * If issue is an infrastructure issue, then it has to be solved by the Supplier.    * If the issue is an external service issue, the Supplier has to inform the relevant Eskom Supplier, where after it will be solved by the relevant Eskom Supplier.    * If the issue is an application level issue, then Supplier will assist to identify and implement quick turnaround solutions (a work around) on the infrastructure support side (i.e. a turnaround activity that requires less than 2 (two) hours of effort typically). If this is not possible, the troubleshooting activity will be closed. Eskom may then have to request a Change Request to deliver the intermediate fix under the Change Management Procedure. Eskom may, however, still require expertise and assistance from the Supplier to support more complex troubleshooting. | R, A | I |

## Information Security Management Services

Information Security Management Services provide security related services that cut across an organisation’s business and IT environment to help safeguard and maintain the confidentiality, integrity and availability of information. This section should be read in conjunction with the agreed RASCI.

* The Patch Management Service provides for the distribution, management, monitoring and feedback function of patch updates throughout Eskom’s IT infrastructure environment. This Service applies to the server operating system level.
* The Anti-Malware Management Service provides for the distribution, centralised management, monitoring and feedback function of anti-malware signature files and updates throughout Eskom’s IT infrastructure environment.. Anti-malware includes, but is not limited to Anti-virus, Host Intrusion Detection and Prevention System, Host-based firewall and advanced persistent threat protection.
* The Vulnerability Management Service provides for identification, classification, remediation and mitigation of vulnerabilities.
* This Service should also provide for expert consultation by the Supplier in respect of the various Information Security Services offered by the Supplier in its security catalogue.

Table 9: Information Security Management Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Patch Management Services Roles and Responsibilities** | **Supplier** | **Eskom** |
| 1. Identify, test and apply OS patches (both security and critical patches) and firmware updates according to Eskom Policies. | R,A | I |
| 1. Track the rollout process of patches in the Eskom OS environment to ensure successful deployment. Provide for a roll back of patches if the new deployment fails. Provide feedback. | R,A | C,I |
| 1. Update the baseline of patches, and make the baseline available for the implementation of new devices. | R,A | I |
| **Vulnerability Management** | **Supplier** | **Eskom** |
| 1. Scan environment to identify the vulnerabilities. Report and remediate vulnerabilities as per an approved remediation plan. | R,A | I |
| **Anti-Malware Management Roles and responsibilities** | **Supplier** | **Eskom** |
| 1. Configure the relevant technologies in Eskom’s environment, for the Anti-malware Management Service in accordance with Eskom's Information Security policies and procedures. | R | A,I |
| 1. Ensure that anti-malware Software Services are operational in Eskom’s server environment. | R | A,I |
| 1. Configure the anti-malware Software policy to optimise the functionality of the application. | R | A,I |
| 1. Deploy the anti-malware signature files in line with the anti-malware Software policy to the server environment | R | A,I |
| 1. Monitor the distribution of anti-malware signatures in the server environment of Eskom | R | A,I |
| 1. Monitor the virus activity in the server environment | R | A,I |
| 1. Monitor the connection of the server devices on behalf of Eskom. Detect devices connected that do not conform to Eskom standard, which are not contracted, when detected. | R | A,I |
| 1. Intrusion detection and Protection Monitoring: Eskom must ensure that the wider infrastructure is protected. | I | R,A |
| 1. Identify uninstalled anti-malware Services in the server environment on behalf of Eskom. | R,A | C |
| 1. Identify unsuccessful anti-malware signature updates in the server environment. | R,A | C |
| 1. Manage anti-malware administrator servers on behalf of Eskom. | R,A | I |
| 1. Remedy virus infection and uninstalled anti-malware Services by reinstalling anti-malware Services and updating signature files. | R,A | C |
| 1. Firewall Installation and Management: Eskom will provide and manage this capability within the environment. | I | R,A |
| 1. Security Specialist Consulting: Provide Information Security Specialist Consulting Services to Eskom in accordance with the agreed Schedule or Appendix for same (If requested by Eskom). | R,A | C |
| **Logical Access Management Roles and responsibilities** | **Supplier** | **Eskom** |
| 1. Securely manage the lifecycle of logical access accounts on the host environments using the Least Privilege Principle. | R, A | C, I |
| 1. Suspend/Delete dormant and rogue logical access accounts on the host environments. | R, A | I |
| 1. Report on account status (created, suspended, deleted) on the host environments. | R, A | I |
| 1. Provide host activity logs insofar as it relates to the confidentiality, integrity, availability and auditing of Eskom’s environment. | R, A | I |
| **Secure communications** | **Supplier** | **Eskom** |
| 1. Encrypted channels must be provided to protect Eskom administrator and user communications against unauthorised access. | R, A | S, C |
| 1. Hardening of administrator end-user devices (eg. laptops) and/or intermediary management devices used to manage the host environments that support Eskom’s infrastructure environment. | R, A | C,I |
| 1. Backups of the hosts and the Virtual Machines must be encrypted to comply with Eskom’s Encryption Standard. | R, A | S, C |

## Configuration Tracking

Configuration tracking service includes all the activities needed to ensure that Infrastructure assets and their configuration are properly tracked.

Table 10: Configuration Track Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Configuration Tracking Roles and Responsibilities** | **Supplier** | **Eskom** |
| 1. Ensure that the CMDB is maintained with all infrastructure CI information and provide hardware and software configuration detail reporting. | R, A | I |
| 1. Install and manage software license usage reporting agents (provided by the Cross Functional Supplier). | R, A | I |
| 1. Provide the history of changes and revisions of total infrastructure environment. | R, A | I |

## Capacity and Performance Management

Component and Capacity Management service aims to ensure that the capacity and performance of services running on the infrastructure platform can deliver in accordance with the agreed Target Service Levels in a cost effective and timely manner, within the agreed Performance Standards. Eskom requires component level capacity and performance management to cover CPU, Memory, Network, etc.). The Supplier will provide the Cross functional Supplier with this capacity and performance information for planning and reporting.

Table 11: Capacity and Performance Management Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Capacity and Performance Management** | **Supplier** | **Eskom** |
| 1. Manage infrastructure platform utilisation in order to ensure that available spare capacity is maintained for future growth (especially for virtualized environments) | R, A | I |
| 1. Manage and maintain performance of physical and virtualised environments effectively within the agreed Performance Standards. | R, A | I |

## Customer Satisfaction

The Supplier shall implement a process to manage customer satisfaction which includes, but not limited to, the following roles and responsibilities:

Table 12: Customer Satisfaction Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| Customer Satisfaction Management Roles and Responsibilities | Supplier | Eskom |
| 1. Review the customer survey results | R, A | I |
| 1. Provide and implement a service improvement plan to address gaps and improve customer satisfaction levels | R, A | I |
| 1. Provide feedback to the Eskom on the steps taken towards improving customer satisfaction levels | R, A | I |

## Disaster Recovery Services

Disaster Recovery Services and IT Service Continuity are the activities associated with providing prioritised IT Service Continuity and Disaster Recovery Services for Eskom applications in respect of the infrastructure associated to the applications i.e. servers, storage/data and backup infrastructure.  The Supplier will provide Disaster Recovery Services according to Eskom’s Disaster Recovery Plan, in respect of the infrastructure under the Supplier's control.

Eskom has an internal Disaster Recovery team that manages the Disaster Recovery function for Eskom systems and required the following DR services from the Supplier to support the DR function:

* Development and maintenance of a Disaster Recovery Plan is done by the Eskom DR team however the execution of the plan during an actual Disaster or DR test is a requirement from the Supplier, as well as the provision of technical information for the development of the plan.
* Disaster Recovery testing coordination is done by the Eskom DR team however, assistance and participation with testing is required from the Supplier.

# Inclusions

This section specifies those activities associated with the infrastructure support, that are deemed included with the services required by Eskom.

* Eskom’s Operation Technology (OT) infrastructure will require technical support.
* Installation and configuration of environments in scope.
* Eskom may require the Supplier to supply the hardware and Spectrum software for the SAP backups. The Supplier may be required to purchase the exiting SAP backup hardware, refresh it when necessary and provide it back to Eskom as a service. Please supply pricing to show support costs for these backups and include a separate view for the hardware and Spectrum software cost. Eskom will have the option to supply this software itself or opt for the Supplier to supply this software.
* Eskom has infrastructure located countrywide that are supported by our two IaaS service providers. Eskom has IT solutions deployed on infrastructure that spans across the locations e.g. solutions are deployed on infrastructure located in central region are linked to infrastructure located in the regions. Due to the solution architecture, the various IT service providers are expected to collaborate with each other for server, storage and backup related matters.
* The Cross Functional Services Supplier is dependent on input from the IT service providers to deliver on their mandate. The Supplier will therefore provide assistance to the Cross functional Supplier for the following:
* Input to Service Improvement Plans.
* Delivery on Adhoc reports when requested.
* Report on recalls for resolved Incidents.
* Report on the number of incidents caused by change requests.
* Update information about Problems, workarounds and resolutions in the Knowledge Management System and the Known Error Database.
* Report on the number of incidents caused by threshold breaches relating to capacity and performance management.
* Eskom will also require ad-hoc services from the Service Provider. The following list of ad-hoc services should be provided, including but not limited to:
* Install X86 Server (Windows, Linux etc)
* Install master installation version (e.g. IBM, NIM server)
* Install UNIX Server
* Create virtual server (Windows)
* Create virtual server (Linux)
* Create virtual server (Oracle OVM)
* Create virtual server (UNIX)
* Create virtual server template (Windows, Linux etc)
* Physical to Virtual migration
* Virtual server host build X 86
* Virtual server host build RISC
* Setup and configuration of storage
* Setup and configuration of backups
* Setup and configuration of restores
* Movement of hardware between locations

Costs for the ad-hoc services above are non-committal and will only be paid when services are rendered.

# Exclusions

This section specifies those activities associated with support, that are excluded from the services required by Eskom. All standard support related activities NOT listed below shall be deemed to be included within the scope of the support services required by Eskom.

The following items are specifically excluded from this SOW:

* Application installation, support and management (however, assistance with server/OS related tasks for application is included). This is an internal Eskom function.
* Database creation, support and management (however, assistance with server/OS related tasks for databases is included). This is an internal Eskom function.
* Development and maintenance of a Disaster Recovery Plan (however, the execution of the plan during a Disaster or DR test is included, as well as the provision of technical information for the development of the plan). Eskom has an internal Disaster Recovery team that manages this service.
* Disaster Recovery testing coordination (however, assistance with testing is included)

# Appendices

* Appendix A – Environment Overview
* Appendix B – Service Level Requirements
* Appendix C – Cross Functional Cloud Services SOW