NKANGALA DISTRICT MUNICIPALITY

PROJECT 118326: APPOINTMENT OF A SERVICE PROVIDER FOR PROVISIONING OF DISTRICT-WIDE ICT DISASTER RECOVERY AS A SERVICE (DRaaS) FOR A PERIOD OF 36 MONTHS

SCOPE OF WORK

Part C3: Scope of Work

C3 Scope of Work

NKANGALA DISTRICT MUNICIPALITY

PROJECT 118326: APPOINTMENT OF A SERVICE PROVIDER FOR PROVISIONING OF DISTRICT-WIDE ICT DISASTER RECOVERY AS A SERVICE (DRaaS) FOR A PERIOD OF 36 MONTHS

1. INTRODUCTION

The Nkangala District Municipality is a Category C municipality in the Mpumalanga Province. It is one of the three districts in the province, making up 22% of its geographical area. It is comprised of six local municipalities: Victor Khanye, Emalahleni, Steve Tshwete, Emakhazeni, Thembisile Hani, and Dr JS Moroka. The district's headquarters are in Middelburg. Nkangala is at the economic hub of Mpumalanga and is rich in minerals and natural resources. For more information on the company, you can visit our current website: www.nkangaladm.gov.za

2. BACKGROUND

Over the years, NDM has made significant investments to put in place standard processes and infrastructure that will ensure efficiency in its operations. This increased dependency on technology coupled with an expansion in the scope and volume of services, business processes, transactions and regulatory requirements has created an increased risk of disruption to normal services. Unforeseen incidents ranging from natural disasters, hardware failure, and information security breaches can have an adverse impact on a business and prevent it from continuing normal services.

To this end, NDM has implemented Business Continuity Management hat aligns with the globally recognized ISO 22301, Business Continuity Institute Good Practice Guidelines, ISO 31000 and King IV. The BCM process encompasses emergency response, crisis management, business recovery and disaster recovery.

One of the key pillars of the BCM is IT Disaster Recovery (DR). In terms of the Business Continuity Management (BCM), It is expected that Information and Communication Technology (ICT) implement recovery strategies to ensure that IT Services, Systems, Infrastructure, Hardware, and Software can be recovered within the Organisation's recovery requirements, specifically Recovery Time Objective (RTO) and Recovery Point Objective (RPO). To this end, ICT seeks to implement the IT Disaster Recovery for its Primary ICT Infrastructure as well as build and cater for the Local Municipalities in the Region.

3. IT LANDSCAPE

NDM ICT infrastructure is on-premises and fully virtualised on VMware platform located on one site in Middelburg, Mpumalanga. The infrastructure consists of the following:

3.1 Primary site

3.1.1 Hardware

The system consists of the following components:

- Host (HP 3x ProLiant DL380 Gen9) with 52 Virtual Machines Running;
- 53.36TB Total SAN capacity (with 34.8TB used) ;
- 220.51Ghz CPU capacity (with 20.46GHz used);
- 1.5TB RAM (with 437.93Gb used);
- Cisco Fire Power Firewall;

3.1.2 Core IT Infrastructure applications

NDM SOC IT Infrastructure use the following applications:

- Microsoft Windows Server 2016 Active Directory
- VMWare 7.0
- A total of 80 Virtual Machines running various Operating Systems (Windows Server 2008, 2012, 2016, 2019, and Linux)
- Microsoft Exchange server 2016
- Mimecast email security and cloud-based archiving
- Veeam Pro back-up and replication
- Kaspersky Endpoint Management.

3.1.3 Networking

NDM SOC IT Network Infrastructure has the following components:

- Multiple VLANS (Voice, Server, Guest Wireless, Employee's Wireless, Workstations);
- MTN APN Connection

3.1.4 Business Applications

- Cisco VoIP Telephone System
- Sage VIP Premiere HR and Payroll
- SQL Server (2014, 2016, 2019)
- TeamMate
- Manage Engine
- Munsoft
- Microsoft 2016 and 365 Office
- Kaspersky Anti-Virus.

3.2 Backups

NDM IT currently performs backup using Veeam:

- Incremental backups to disk are done daily
- Full backups to disk are done once a week
- Weekly tape archiving is done and sent offsite
- Monthly tape archiving is done and sent to offsite

THE BIDDER MUST PROVIDE A CLOUD BASED DISASTER RECOVERY SOLUTION THAT WILL HOST 6 MORE LOCAL MUNICIPALITIES DATA AND INFRASTRUCTURE OF A SIMILAR SIZE AS SPECIFIED ABOVE. THE PROPOSED SOLUTION DESIGN MUST ACCOMMODATE THE REQUIREMENT.

4. THE SCOPE

4.1 FULL DR REPLICATION ON THE CLOUD / DISASTER RECOVERY AS A SERVICE (DRaaS)

NDM seeks to appoint a service provider for a period of three (3) years to provide recovery of its data center services in an efficient and economically advantageous way, with minimal data loss/downtime and a rapid recovery time, as stipulated within the BCM for Recovery-Point Objective (RPO) and Recovery-Time Objective (RTO) tailored to meet ours and the Local Municipality's specific requirements, to be included into the Service Level Agreements (SLA).

The Disaster Recovery as a service (DRaaS) should replicate infrastructure, applications and data to the cloud to serve as a secondary site and enable full environmental recovery in the event of a disaster.

The cloud secondary site must effectively become the new environment and allow NDM and associated local municipalities to continue with daily business processes while the primary system undergoes repairs.

4.2 REQUIREMENTS

4.2.1 DRaaS Requirements

- Rapid, effective, and testable recovery of targeted systems, services, or data in a declared disaster or when the primary site goes offline:
- Readily and repeatedly testable at minimal or no cost,
- Testable during regular business hours with minimal or no impact to production systems, services, or data.
- Recovery Point Objectives (RPO's) of 4 hours or less (as specified in the BCP)
- Recovery Time Objectives (RTO's) of 4 hours or less (as specified in the BCP)
- Full replication in the Cloud and distribution of the traffic between the on-premises site and cloud environments to allow NDM to recover.
- In the event of a disaster or an emergency that causes NDM's on-premises environment to go offline, the solution must route all NDM's traffic to the cloud setup and scale appropriately.

The DR solution at a minimum must have:

- The ability to automatically backup critical systems and data,
- The ability to quickly recover from a disaster, with minimal user interaction,
- Flexible recovery options, such as restoring a single application or the whole infrastructure,
- Heterogeneous Application-aware replication (Windows/Linux/UNIX Guest VMs)
- Partial Failover/Failback scenarios must be supported
- End-to-end AES 256-bit encryption with built-in compression
- Disaster Recovery self-service testing, on-demand
- DRaaS management model: This must be a fully managed service

Where the winning bidder takes overall responsibility for the planning, testing and management of disaster recovery, with some flexibility to allow NDM's involvement throughout the process, as and when it deems it necessary, the following will form part:

- A DRaaS subscription model is desired
- Preserve current VLANs configuration for easier failover
- Provide 4 disaster recovery tests per annum
- Provide both guest and business wireless infrastructure configured to work with DR infrastructure
- Provide pricing schedule according to RPO and RTO with proposed Service Level Agreement (SLA)
- The winning bidder will be responsible for replication schedule
- The winning bidder will be responsible for managing the link between NDM's premises to the DR

- The winning bidder must have the hosting data centre infrastructure located in the borders of South Africa boarders to ensure that data is stored and processed within this country for compliance reasons
- The hosting clouds must be available to each other to ensure adequate service continuity

4.2.2 Implementation Requirements

- Provide key personnel who will be responsible for the implementation of the project and determine the roles, responsibilities, and the team structure of such personnel. All key personnel dedicated to the project shall be properly qualified, possess valid certifications issued by the relevant vendor (if any)
- Document IT Disaster Recovery Strategy
- Document IT Disaster Recovery Plan
- Document IT Disaster Recovery Procedures
- Test of IT Disaster Recovery and signoff

4.2.3 Information and data security requirements

Strong Encryption Provides the Necessary Protection

The first line of defense for data is robust, 256-bit AES encryption. All data must be encrypted whether it is at rest or in transit between NDM and DR site.

Control of encryption keys

NDM desires to have exclusive control over its data. To this end, NDM will engage the winning bidder and agree an arrangement for the control of encryption keys:

- Municipal data must be securely stored and hosted within the Republic of South Africa's borders.
- The service must be able to protect public IP addresses against layer-4 to layer-7 distributed denial of service (DDoS) attacks and sends alarms immediately when detecting an attack.
- The service must be able to provide identity authentication and permission management.
- The service must support fine-grained access control for the cloud resources.

4.2.4 Service Level Requirements

- Recovery Point Objectives (RPO's) of 4 hours (As stated in the BCP)
- Recovery Time Objectives (RTO's) of 4 hours (As stated in the BCP
- Four disaster recovery tests per annum
- Bidder must coordinate the annual review and sign-off of the IT Disaster Recovery Strategy
- Bidder must coordinate the annual review and sign-off the IT Disaster Recovery Plan
- Bidder must coordinate the annual review and sign-off IT Disaster Recovery Procedures
- Frequent reporting and management visibility through an online portal,
- Daily, weekly and monthly reports to be provided regarding replication status
- Alerts on replication failures.

4.2.5 Other requirements

Given the critical nature of the recovery of NDM's and the associated local municipality's data should the need arise; there are a number of requirements that the winning bidder must provide for:

- Adequate bandwidth for the replication as well as access to the DR in the cloud
- All-inclusive pricing
- The DraaS solution must incorporate file size management to reduce storage needs
- Failover assistance in a moment's notice
- NDM's active involvement in DR testing.

4.3 Compulsory requirements

- The winning bidder will be responsible for managing the link between NDM's premises to the DR
- The winning bidder must have a hosting data centre located in South Africa
- The winning bidder must have multiple data centres for redundancy and failover purposes.

5. DELIVERABLES

5.1 Implemented Cloud Disaster Recovery solution
5.2 IT DR Plan
5.3 IT DR Strategy
5.4 Disaster Recovery Testing
5.5 Disaster Recovery Procedures

6. PRICING

- All-inclusive pricing
- Subscription model
- Show monthly or annual costs, inclusive of VAT

6.1 Pricing Phase based

All costing must be modeled under the following two Phases;

6.1.1 **Implementation (Phase 1)** – to include all under design & implementation as a once-off phase and not limited to;

- Traveling cost to all sites (Main offices of all Municipalities in the Nkangala region)
- Preparation of the Cloud platform and Tenants
- Data & environmental assessment, including the migration to the cloud

6.1.2 **Subscription (Phase 2)** – to include all relevant items for the full functionality of the platform and not limited to;

- Backup and replication of the Platform
- Support and Maintenance of the Platform
- All relevant software and resources for the adequate functionality of the solution as a Disaster Recovery as a Service (DRaaS)