Nkangala District Municipality

OPEX Business Solutions (PTY) LTD

E-Procurement System

Dedicated Cloud Server

12th MARCH 2020

2020

Nkangala District Municipality

SECURITY REVIEW APPROVAL

LIVE DOCUMENT

OPEX
Business Solutions (PTY) LTD

Contents

OPEX
Business Solutions (PTY) LTD

Version History

This development and distribution of the technical review is a summary of the evidence file that contains sensitive information about the project details and user administrations.

The Intended persons, whom are allowed to review the document are for the sole purpose of a super user and representative of Nkangala District Municipality

Version Number	Created By	Revision Date	Approved By	Approval Date	Description of Change
1.1	Antonio Pisapia	6th March 2020	Antonio Pisapia		Document Creation
1.2	Kamogelo Molotsi	12th March 2020	Antonio Pisapia		Document Amended for Application Security

Stage Gate 1
Cloud Server Setup
Installation of Environment Dependencies
SSL Certificate
Auto-Deployment

STAGE GATE 1

Item	Deliverables	Status Review	Review Y / N
1	Cloud Server Setup	A dedicated cloud server has been purchased and implemented with the domain : https://nkangala-scm.online	
2	Installation of Environment Dependencies	All server dependencies where the application is deployed are installed on the server.	
3	SSL Certificate	SSL certificate has been implemented to keep sensitive information sent across the Internet encrypted : https://nkangala-scm.online	
4	Auto-Deployment	pending	

Reviewed By:

Comment:

_____

_____

_____

_____ Date: _____

Supply Chain Rep (Name and Signature)

Comment:

_____

_____

_____

_____ Date: _____

ICT Representative (Name and Signature)

Comment:

_____

_____

_____

_____ Date: _____

SCM Manager (Name and Signature)

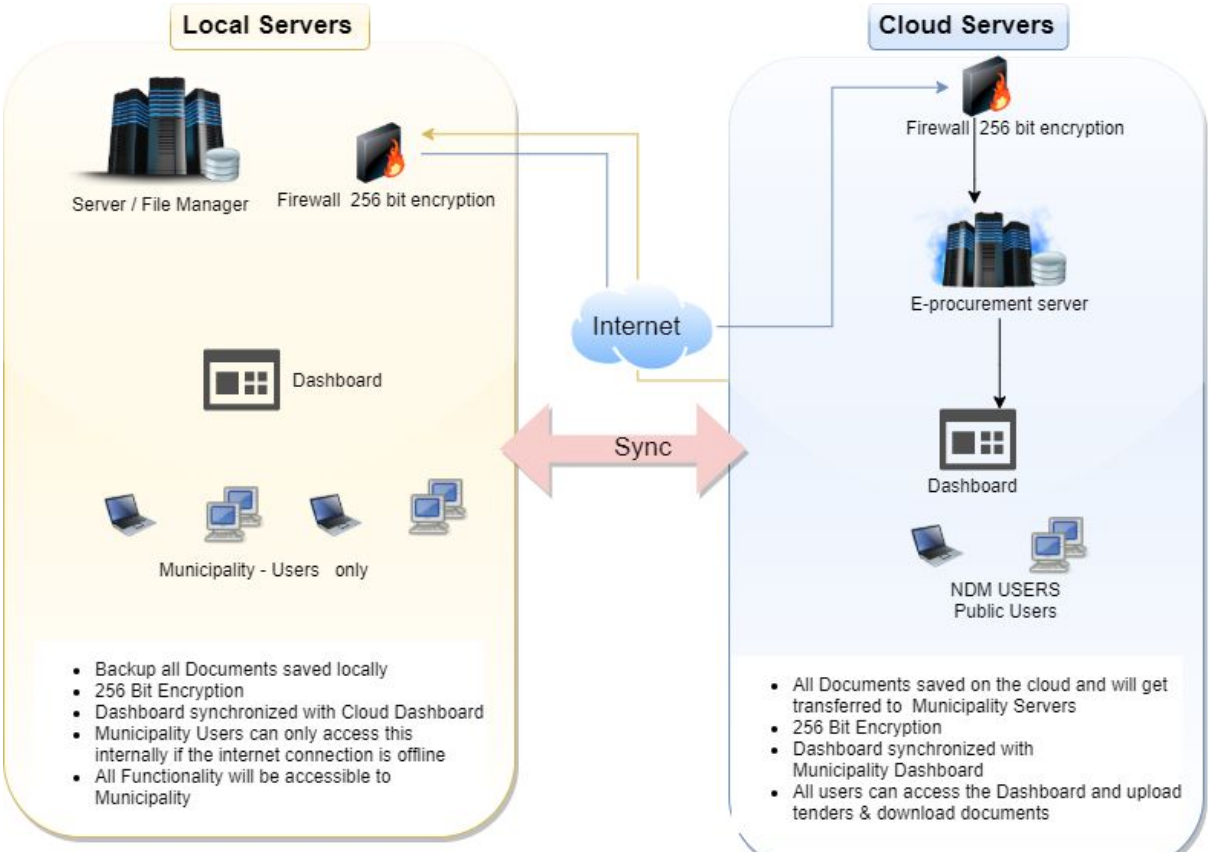
Statement of Need

Nkangala Municipality District is looking to enhance its supply chain management capabilities. In this regard, they are looking at implementing an e-Tender application which will help them manage the end to end workflow of the tendering process.

To mitigate risk, a dedicated cloud server is required to allow multiple entry points of traffic to engage with the E-procurement service. Once data has been captured, the Local server at Nkangala District Municipality will sync all available data from the dedicated cloud server and keep a local copy.

Should the dedicated server go down due to internet, DNS or Fibre link outage, the Local Server at Nkangala Municipality will have a functional Replication of what was on the Dedicated server, thus allowing no loss of information or downtime for the Municipality.

Cloud Server Architecture



Local Servers Requirements

- Linux OS (LTS) Ubuntu
- 12GB RAM DDR4
- 30 TB Storage expandable
- 100/1000 Ethernet

Dedicated Server Security Checklist

1. Monthly Server Software Updates
   - Run manual package updates, or if you are going to run updates.
   - Log Review on processed updates
   - WHM access and Remote Sync from Server to Local Server at Nkangala

2. Controlled Software installation.
   - Git Version Control
   - Composer (Dependency Package Manager with SSH Access)
   - PHP Artisan (Generate Broken Source Code Files for Zero Downtime)
   - Auto-migrations for Database Deployment
   - Laravel Zero Downtime Auto-Deployment Environment

3. Secure SSH and Remote Access
   - SSH port change
   - Disabling direct root login
   - Restrict access to certain IP's
   - Using SSH Keys instead of passwords to secure SSH access

4. Maintain and Secure Database Areas
   - SQL injection protection and tests
   - Minimized Privileges to database users
   - Deleting unneeded Data in database
   - Avoiding Database interactions where it's not required
   - MariaDB will be used for large entries
   - Faster Indexes/Cache: When using the MEMORY storage engine, MariaDB can complete INSERT statements up to 24% faster than traditional MySQL servers, along with CHECKSUM TABLE and MyISAM Segment Key Cache being 4x faster

5. Maintained Server Backups
   - Multiple backups kept on dedicated server
   - Multiple backups synced to Nkangala Data Centre
   - Multiple restore points
   - Secured at Bryanston's NOC Centre
   - IDC access required if technician needs to get to site which requires 24hrs notice
   - Second HDD for storage of Database and Files uploaded at NOC
   - Second HDD for storage of Database and Files uploaded and synced to Nkangala Data Centre
   - Multiple backup restore points done at a incremental Backup
   - Ability to restore Database , and Files kept at a 24-36 hrs roll back
   - RAID 5
   - Linux environment - no malware – no viruses, no rootkits

Reliable Infrastructure

Your servers will be securely hosted at state-of-the-art data centres. These facilities provide redundant power, fire suppression and excellent physical security.

Managed Hardware
MTN NOC uses the latest rack-mount servers with Xeon processors and ample RAM depending on your requirements. MTN NOC will ensure that the hardware is maintained and will be responsible for any hardware issues

Locally Hosted
Our servers are hosted locally, which means that you and your users will get the fastest connection to your website. With a 99.8% uptime

Fast and Reliable Network
Your servers will be hosted at the hub of South Africa's online community, with redundant links to international audiences.

Managed Services

OPEX and Afrihost will manage the physical environment, network, hardware and operating systems, leaving you to concentrate on your applications and data.

Server Information

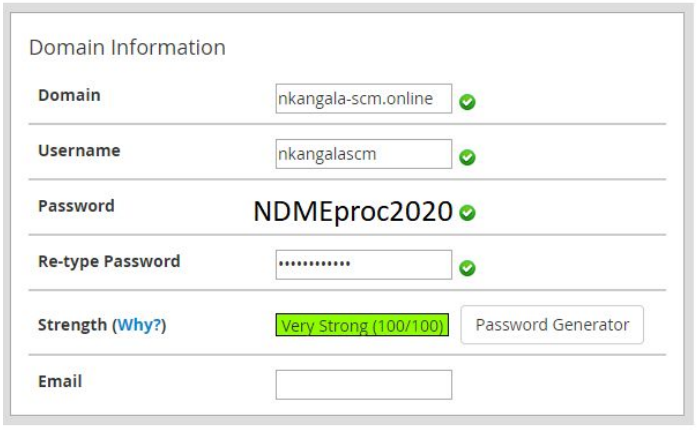
Server Information	Details
OS	CentOS and CPANEL Managed
Hostname	eproc.dedicated.co.za
Dedicated IP	41.76.212.84
Gateway	41.76.208.1
Netmask	255.255.248.0
DNS Servers	197.242.155.155 197.242.144.144
WHM ACCESS	**Details**
URL	http://eproc.dedicated.co.za:2087
Username	eprocdbx
Password	fc507xqgMlut
SSL Certificates	Enabled
Installed	CPanel Stable
Server Type	Managed

Server Specifications

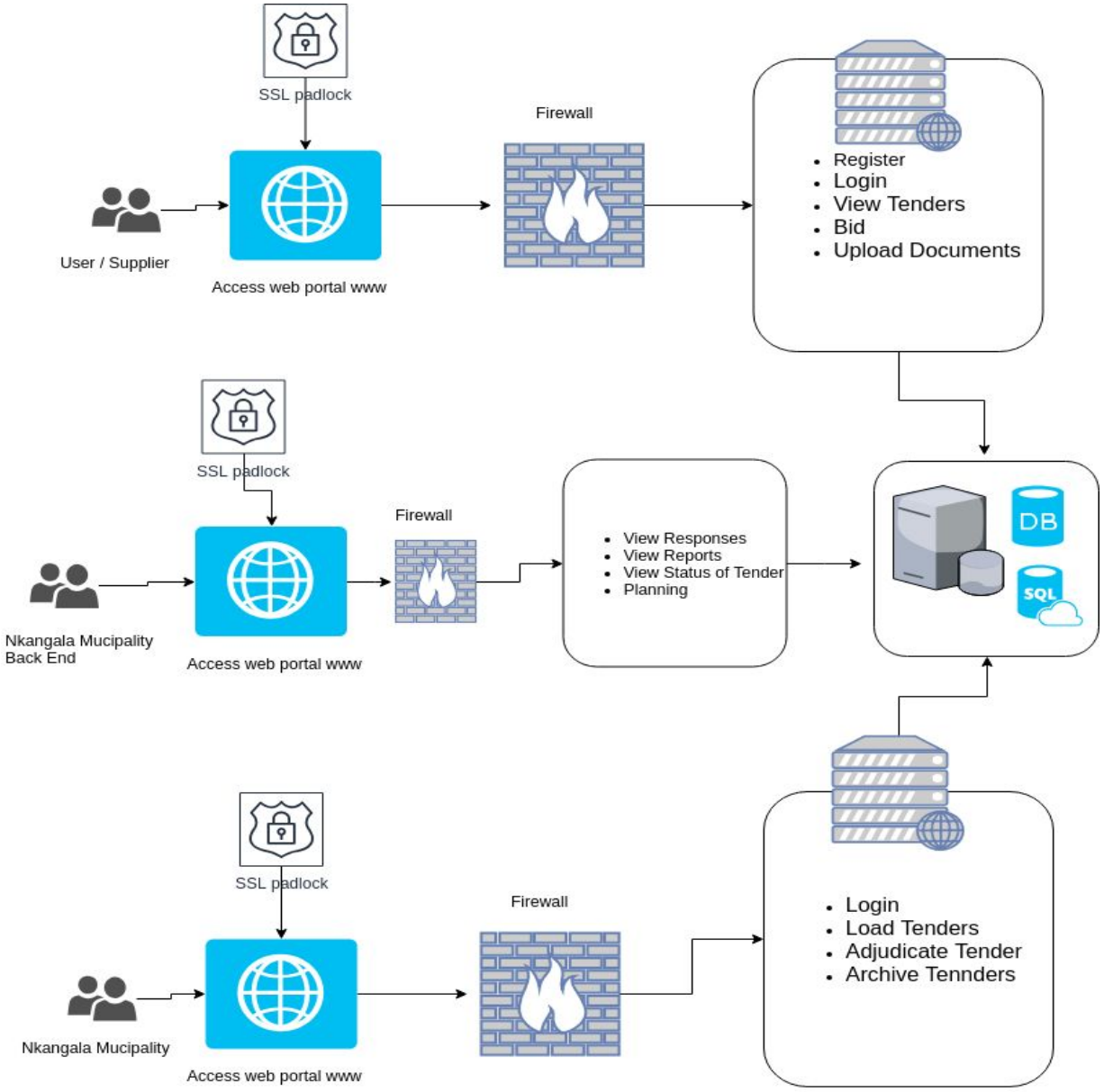
Server Info	Details
CPU	3.2GHz Quad-Core Xeon [redacted]
RAM	8-32GB
Hard Drives	3x 1TB
RAID Level	Raid 5
Web traffic	10TB pm

OPEX
Business Solutions (PTY) LTD

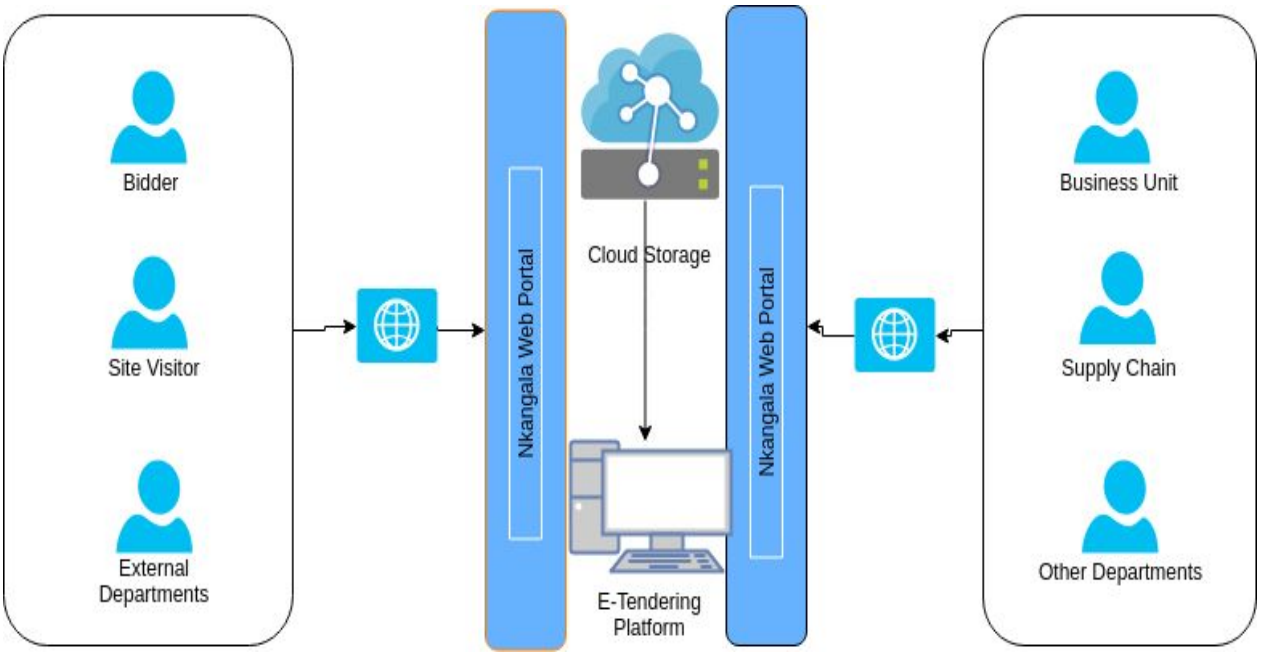
Domain Access Details for E-procurement



Framework of E-Tendering



Business Requirements



Security Requirements

To meet the industry enterprise application standards, the E-Procurement system is built on a LARAVEL framework (version 5.8), a very secure and stable enterprise application framework that supports and implements high encryption authentication and authorization modules.

Laravel comes shipped with core security packages and features that have been successfully implemented on the E Procurement for a more controlled and secure public web environment. Other security mitigation measures implemented on both the public portal (public suppliers) and admin portal (NDM internal staff) are :

- **Authentication System**
- **CSRF (Cross Site Request Forgery)**
- **SQL Injection**
- **Re-Capture (Password Authentication)**
- **MVC Support Design**

Authentication System

We've implemented a robust user authentication process in place with the associated security modules available in Laravel. Implementation of "providers" and "guards" to facilitate the authentication process. The purpose of "guards" is to authenticate users for each request they make, while "providers" facilitates to retrieve back the users from the database. This insures a very secure request/response communication between any device running the E Procurement System and the server that is serving the application.

CSRF (Cross Site Request Forgery)

To protect the system from forged requests, we have implemented CSRF tokens to make sure that external third parties cant generate fake requests and should not breach the system's security vulnerabilities. For this, Laravel creates and integrates a valid token into every request that comes from a form of through an AJAX call. When the request is invoked, Laravel compares the request token with the one saved in the user's session. If the token does not match, the request is classified as invalid and no further action is executed.

SQL Injection

For all SQL statements and connections we're using the Fluent Query Builder / Eloquent.If hackers add a new input to a form, they may try to insert a quote and then run their own custom SQL query to damage or read your application database. However, this won't work since we are using Eloquent. Eloquent is going to escape this SQL command and the invalid query will just be saved as text into the database.

Password Protection

During the Registration / User creation passwords are not saved as plain text. they are hashed instead, which means transformed into a random string of characters unreadable by hackers and even system administrators. The two major Laravel security facades we implemented in user password hashing are Bcypt and Argon2. Unlike other forms of encryption, hashes are not designed to be decrypted with any key. this is "one way" action. When a user enters a password again, its hash is verified against the one received previously.

Re-Capture (Password Authentication)

In most cases intruders uses bots / scripts, and other forms of automated attacks to gain access to the systems, with reCAPTCHA inplace chances of them succeeding are minimized drastically, reCAPTCHA requires some sort of human input, the one we've implemented on this system asks a user to select a certain picture the list, if they get it wrong they won't be able to proceed with the logging in or registration process.

MVC (Model View Controller) Support Design

Model-View-Controller (MVC) architecture maintains clarity between application logic and presentation by isolating the application views from the actual application code that runs in the background. It enables optimum performance and proper documentation. The multiple functionalities of MVC enable a modular design approach to developing robust independent modules which are easily maintainable and deployed. The implemented MVC model :