devman3
Information for growth.

# Technical & Security Information

IS Kidz Africa (Pty) Ltd | +27 (0)21 422 3627 | www.devman3.com | support@devman3.com
408 The Studios, 112 Buitengracht Street, Cape Town 8001
Company Registration No. 2003/013742/07 | VAT Registration No. 4530209321

# Table of contents

The DevMan application is Software-as-a-Service (SaaS). DevMan is available over the internet and is secured with SHA-256 signed encryption SSL certificates and TLS1.2 protocol.

We endeavour to follow industry standard best practice.

This document outlines:

- System access
- User hardware and network requirements
- Physical infrastructure
- Cyber security
- DevMan communications
- Data security FAQ's

# System access

Each specific instance of DevMan is associated with a unique URL to the login page.

Users have their own unique login name, individual (encrypted) passwords can be managed and updated by the user once logged in. Multi-factor authentication is also available, on request.

Access to DevMan is granted on request by an authorised person.

Once access is gained, a second layer of security can limit access to different modules and the amount of data they can change or see.

# User hardware and network requirements

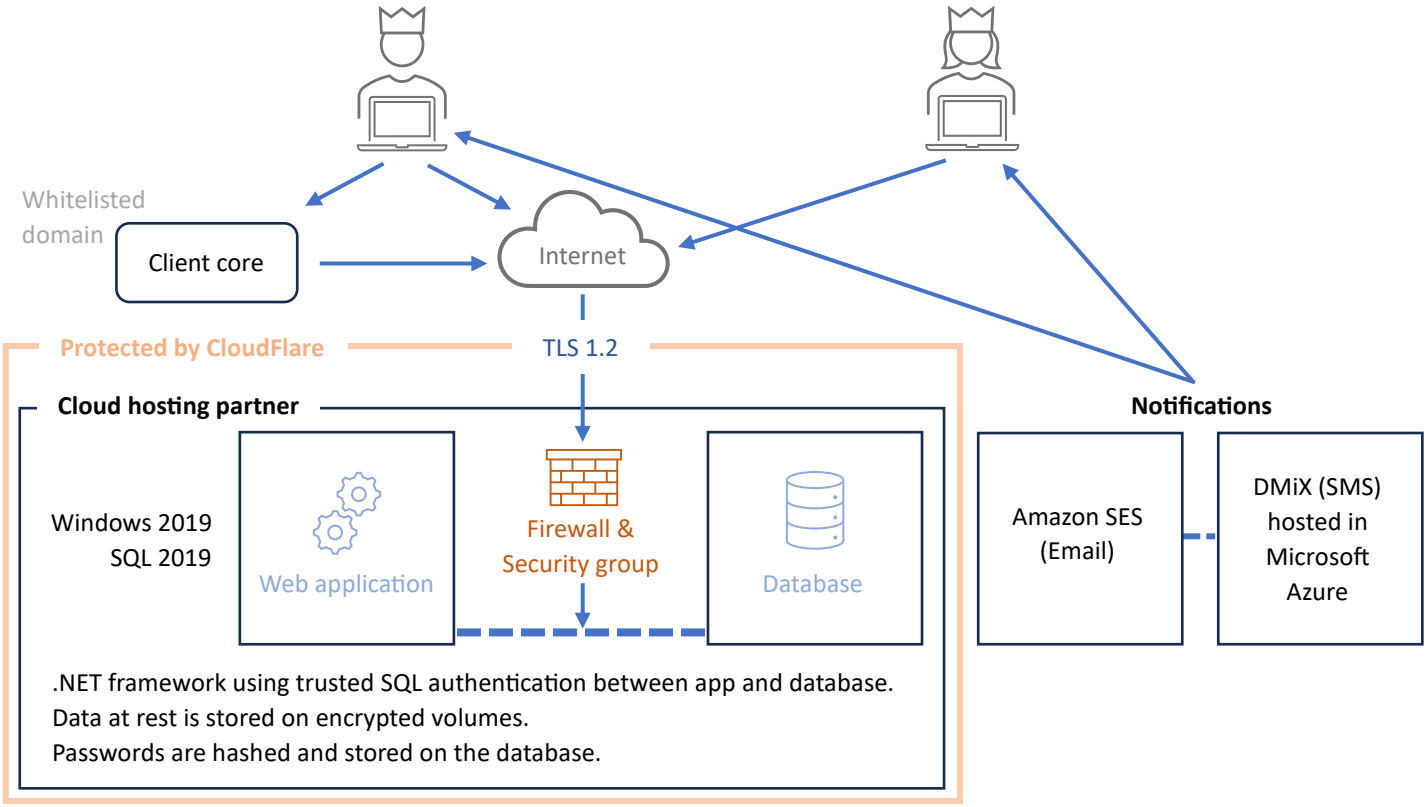
Network bandwidth plays a very important role and needs to be matched with server performance to optimise user experience. User hardware and software minimum requirements are:

| Minimum hardware | Software |
|---|---|
| Intel i5 processor or higher | Windows 10 or higher<br><br>Microsoft Word and Excel 2013 or higher |
| 8GB RAM | DevMan is tested for current W3C compliant mainstream browsers, namely Google Chrome, Microsoft Edge, and Mozilla Firefox.<br>**Note:** Internet Explorer is no longer supported by Microsoft or DevMan. |
| Internet speed: | Depending on the role and function of the user, internet connectivity should be a stable connection ranging from 2mbps (general user) to 25mpbs (power user). |

# Physical infrastructure

Client applications and their databases are not hosted in-house. We have partnered with Xneelo (Pty) Ltd, a web hosting company based in South Africa. Xneelo delivers service that is reliable and consistent, focusing on infrastructure stability and good value.

Typical DevMan environment:




# Cyber security

Security is a top priority, and several measures have been implemented to protect our systems and our clients' data. No company is 100% safe from an attack or breach, however DevMan undertakes to uphold security standards as best as possible within budget.

These are some of the measures in place:

- WithSecure (formerly F-Secure Business) is a leading security end-point product that includes ransomware protection and patch management. This is installed on all our workstations and servers.
- Encryption – laptop and server hard drives are encrypted, so if stolen they are inaccessible.
- Database backups are encrypted with AES-256 encryption.
- Penetration testing is conducted periodically, and findings are remediated timeously.
- Firewall reviews are conducted regularly along with monitoring software which alerts us to any unusual activity.
- CloudFlare web application firewall secures and ensures the reliability of external-facing resources such as websites, APIs, and applications.
- Password policies are set higher than best practice in the industry.

- Cyber Insurance – our existing policy provides for an incident response team to help remediate and recover as quickly as possible.
- Hardware maintenance – servers are constantly reviewed and maintained at the highest standard possible.

A copy of our Security Incident Policy is available on request.

# DevMan communications

DevMan provides integrated email and SMS communication services for mass constituent communications, event, and marketing campaigns. We integrate with industry leaders ensuring the users benefit from current trends and best practice.

**Email**

Amazon Simple Email Service (SES) to provide reliable bulk email functionality with delivery tracking.

**SMS**

Data Management Integration Exchange, DMIX, (a South African media marketing, strategy, and communications company) provides bulk SMS for text message campaigns.

# Data security FAQ

**General information**

| | |
|---|---|
| User authentication and identity assurance level | Named user with assigned profile role |
| Mean time required to revoke user access | 15 minutes from request and access to system |
| User access storage protection | Salted encrypted password |
| Third party authentication support | DevMan supports LDAP and Azure Active Directory authentication which can be implemented by origin site web-service wrapper. |
| Connection security | DevMan supports industry standard HTTPS encryption, ensuring your data remains private and secure. |
| Database access | Access to the database is only available to users via a DevMan front end application with a unique log in and encrypted password. |
| Database transfer | Our policy is that any portable copies of data need to be on encrypted media. And use FTPS for internal transfers. |

**Will my data be shared with other organisations?**

No, each client has its own discrete set of data separate from all other clients, and access through its' own separate front-end application. Part of the standard SLA is that data always remains the property of the client and is not shared with other organisations. DevMan staff are also required to sign a confidentiality agreement.

**Who has access to my data?**

One or more persons within your organisation will be trained to manage the security within the application (revoking and granting access and assigning roles). Access to the application and database servers is granted to DevMan staff according to their roles and on a need-to-know basis.

**What disaster recovery measures are in place?**

Full SQL server back-ups of databases are performed at several intervals daily and stored in redundant locations.

| | |
|---|---|
| Data Mirroring Latency | Simultaneously (HDD mirror 1 + 0) |
| Data Backup Methods | RAID, SQL backup schedules, script copies to alternate servers, and encryption. |
| Database encryption method | AES-256 |
| Data Backup Frequency | Full database backups 10pm daily followed by differential backups daily every 5 hours. |
| Backup Retention Time | 1 week on-server for daily full and differentials.<br><br>2 weeks off-server for daily full and differentials.<br><br>5 years off-site for Saturday backups. |
| Recovery Point Objective (RPO) | 5 hours |
| Recovery Time Objective (RTO) | 2 days |