System Architecture Overview

Web-Based Application

The system is implemented as a web-based application, eliminating the need for any local software installation on end-user devices. All functionality is delivered through standard web technologies.

Client Access

- The application is accessible from any internet-enabled device via modern, standards-compliant web browsers, including Microsoft Edge, Google Chrome, Apple Safari
- No browser plugins or extensions are required.

Application Framework

- The system is developed and powered by ASP.NET Core, providing:
  - High performance and scalability
  - Cross-platform compatibility
  - A secure, modern application framework supported by Microsoft

Network Security

- All communication between client browsers and the application server is secured using HTTPS.
- Data in transit is encrypted using SSL/TLS certificates, ensuring:
  - Confidentiality of transmitted data
  - Protection against man-in-the-middle (MITM) attacks
  - Compliance with industry-standard security practices

Database Platform

- The backend database is implemented using Microsoft SQL Server, a robust and enterprise-grade relational database management system.

Data Protection (At-Rest Encryption)

- All data stored within the database is protected using encryption at rest, which:
  - Encrypts database files, backups, and transaction logs
  - Prevents unauthorized access to data stored on physical or virtual storage media
  - Supports compliance with data security and regulatory requirements.

North America & Caribbean: (+1) 939.316.4931 – (+1) 407.612.1641
South America: + 57 324.638.1492

Environment

Hosting Platform

The application is hosted on the cloud, protecting your data with geo redundant cloud storage built for backup, archiving, and disaster recovery. Enjoy high availability, durability, and peace of mind knowing your data is always protected and accessible.

Load Balancing

The environment is configured with load balancing capabilities to:

- Distribute traffic across multiple application instances
- Improve system availability and fault tolerance
- Support horizontal scalability during periods of increased demand

Authentication Configuration

The system supports multiple user authentication methods, which may be enabled individually or in combination based on customer requirements.

Local Authentication

- Users may authenticate using locally managed encrypted credentials stored within the system
- Credentials are defined and managed by authorized system administrators

Microsoft Active Directory (AD) Authentication

The system can integrate with Data Protection (At-Rest Encryption)

- All data stored within the database is protected using encryption at rest, which: authentication.
- This enables centralized identity management and policy enforcement.
- The customer must provide secure network connectivity to their AD environment for integration.

Office 365 (Azure Active Directory) Authentication

- The system supports authentication using Office 365 / Azure Active Directory credentials.
- This allows users to sign in using their existing corporate Microsoft accounts
- The customer must provide an Application Key (client ID and related credentials) to enable this integration.

North America & Caribbean: (+1) 939.316.4931 – (+1) 407.612.1641
South America: + 57 324.638.1492