Lokulus provides secure storage and transmission of sensitive data. Access is provided through a combination of data and message encryption, secure messaging, robust security and access control mechanisms.

Security Features

These security features are summarised below:

User Interface – A combination of user authentication, authorisation and fine-grained role based access control means that only designated users can view secure data, and all access to transactional data is logged. Secured data cannot be used in search criteria or results, copied or retransmitted (unless retyped).

Network Security – A combination of Transport Layer Security (TLS) and message payload encryption provides secure system operation and data transmission; payload encryption ensures data security across multiple hops.

Database Security – Database connection details are centrally and securely managed, and all passwords and secured data are stored encrypted within the database.

Encryption Key Management – Encryption keys are centrally and securely managed using multiple keys and multiple levels of encryption.

Secure Data Management – When no longer required, secured data can be automatically deleted and/or obfuscated.

Client Credentials – Client secrets can be stored hashed in the database, which adds another layer of confidence in the system's security.

Identity Service

Vouch our identity service secures the entire Lokulus portfolio of solutions. Extensible for use alongside and external to Lokulus, Vouch provides an enterprise-wide security ecosystem that federates onto common third-party identity providers, such as Microsoft or Google.

Data Access Management

In Lokulus, you can define access rights at various levels. An Agent might have different rights than their supervisor, and other groups of Agents may have additional access rights for different brands.

You can implement Role Based Access Control (RBAC) security measures for a specific user of Lokulus by using three primary mechanisms:

Work Profiles define the user's access permissions to each category of work. Access controls include read, action (update) and auto-offer. As data is always bound to an item of work processed by Lokulus, this mechanism (together with workflow definition) is used to limit access to secure data on a need-to-know basis.

Security Profiles define the user's access to system functionality and, hence, define the user's ability to change system configuration. Security profiles operate at the level of gross access to functionality; object permissions are defined using access control lists.

Access control lists (Owners) – Permissions on any specific configuration object to restrict access to specific user's user groups.. For example, a specific business rule or user group can be modified.

With careful consideration of users and groups, all users need only have access to the data they require to do their job.

For example, agents may not need to see the history events associated with a case, customer or work item. If so, you can set up a profile not to include the history events tab. Their supervisor, on the other hand, might have access rights to see the history events.

A typical set of Groups look like this:

Agents	**Team Leaders**	**Content Author**
Controller	**Administrators**	**Processor**