LOKULUS

PCI Compliance

With attention to proper policies and external factors, Lokulus will help you comply with current PCI data security standards.

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that handle credit card data.

When designing a solution compliant with the PCI standard, of the six principles that it requires that organisations adhere to, two are relevant in this context:

- Protect cardholder data.
- Implement strong access control measures.

Storage of Sensitive Data

All sensitive data is stored securely:

- Secure Storage of Passwords and Data – Passwords for third-party external services requiring encryption are held in a secure encrypted form within the database.
- Obfuscation of Sensitive Data – Where data is extracted from an inbound communication, the obfuscation service will apply the specified obfuscation mask.
- Deletion of Sensitive Data – Data defined as requiring encryption may be automatically deleted (either by a workflow operation or scheduled task) from the work item once the work item/case is closed. Alternatively, deletion of the entire work item (once closed), case and customer can be scheduled as part of the standard archive schedule.
- Client Credentials – Client Secrets belonging to Vouch Clients can be stored as hashed strings in the database.

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.

User Interface

The Lokulus user interface has numerous features around sensitive data that aid in compliance with the PCI Standard. User access to sensitive data is controlled and logged. Sensitive data is also obfuscated, as described above, and can only be transmitted, searched, or stored on the Case or the Customer by users with correct access permissions.

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

- Work Profiles – 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 – 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