

Joven Technology is committed to providing a secure application to our customers. We recognize that the laboratory industry requires secure and reliable systems that will protect the confidential data of its customers. This document provides an overview of some of the mechanisms that we use to protect the Quasar system, your reports, your user information, and your customer information.

Overall Architecture

Quasar is a client-facing system that uses the Internet to interact with your clients. The very nature of the Quasar architecture provides a layer of protection for your internal systems, as your systems are screened from the Internet by Quasar and the security mechanisms described below. All communication with your systems is through a well-defined and secure data feed, inaccessible to any attack from the Internet. Furthermore, your systems “push” data to Quasar, which means that you control what leaves your system.

General Environment

Quasar is based on industry-standard software and hardware, which ensures our ability to extend the product as new technologies are available, and allows us to leverage the extensive investments by industry in the areas of security and scalability. Quasar is built on Microsoft’s SQL Server running on Windows 2000 Server.

Account Management

The Quasar account security model currently provides four types of users (“roles”):

Lab Admin	for lab personnel; can manage all user accounts
Lab User	for lab personnel; can manage client accounts
Client Admin	for lab clients; can manage client accounts
Client User	for lab clients

Lab Users can access most Quasar functions, but only Lab Admins can add, modify, or delete Lab Users. Both Lab Admins and Users can manage accounts for clients. Lab personnel can be assigned to multiple locations, and can be assigned a different role at each location.

Authentication (Passwords)

All users of the Quasar system are required to login using a valid UserID and password. Admin Users can force a user to change their password upon next login, and can control whether or not a user can login at multiple sessions simultaneously. All sessions are automatically logged-out if inactive (length of the Inactivity Timeout is specified by the lab). User accounts can be marked Inactive, which blocks further logins. As an option, we can configure the password selection system to meet your security requirements; for example, require that passwords be a certain minimum length, include both alphabetic and non-alphabetic characters, etc.

Activity Logs

All report accesses are logged by the application. The log includes the User ID, the date/time stamp, and the IP address of the user. If desired by the lab, individuals without a Quasar account can access reports using the “Report Viewer”, which requires only a ReportID and a PIN. Note that the Activity Log will not include the User ID when access is made using the Report Viewer, as there is no User ID.

Report Versions

The Quasar system never modifies or deletes reports which have been added to the system. Any report revisions are stored as another version of the report; earlier versions of the report are retained in the database. By default, only the most current version of a report is viewable.

Client Separation

Quasar maintains a separate set of data for each of your client companies. The internal security provided by the SQL Server database keeps each client company record separate. To ensure accountability by users, each individual at each client company has their own User ID and Password.

Data Integrity

Quasar can store your report in its “native” format (eg, a spreadsheet file), and can optionally convert files to PDF format. PDF files provide a substantial measure of data integrity. As an option, Quasar can provide additional data integrity by adding a digital signature to the PDF conversion process, thereby ensuring that any modification to your report can be readily detected. See our “Application File Types” White Paper for a complete list of files that Quasar can convert to PDF.

Confidentiality / Encryption

Quasar supports the use of the standard “https” protocol, commonly known as SSL, to provide encryption for all traffic to and from the system. The use of this protocol is optional.

Firewall *(applies to hosted systems only)*

The Quasar systems reside behind a firewall to provide a layer of protection from external hosts. This firewall is configured to allow only the traffic required for Quasar. All other network services are blocked by the firewall.

Lab Separation *(applies to hosted systems only)*

Quasar uses a separate database to host each lab, so that there is no co-mingling of your data with another lab’s data. This also allows us to adjust system configuration settings for your database to best meet your specific requirements for security and performance.

Viruses *(applies to hosted systems only)*

Our servers are constantly monitored by industry-leading virus protection software from Symantec, and virus definitions are kept current via automated methods. This software monitors the application-generated files (such as those uploaded by users), all email traffic, and all other file-related activity.

Security Patches *(applies to hosted systems only)*

All security patches are applied, and our staff is automatically notified of any potential security issues. As a member of Microsoft’s Developer Network, Joven Technology has immediate access to all current security and other environmental information. As of this writing, Joven Technology’s servers have not incurred any unscheduled downtime, and have not been affected by any security issues. Our staff is committed to keeping this track record.

Physical Security *(applies to hosted systems only)*

The server systems are hosted at a third-party site, with security measures in-place to restrict access to your data. Only qualified administrators have access to the server systems.

Data Retention *(applies to hosted systems only)*

By default, all system data, including reports, is maintained online for a minimum of twelve months. This period may vary from lab to lab based on individual storage and bandwidth needs. Please contact Joven Technology to discuss your specific requirements.

Backups *(applies to hosted systems only)*

Joven Technology performs regular backups of the system to ensure that your data and reports can be recovered in the event of unforeseen events. Off-site storage of backup media ensures that your data will survive complete destruction of the hosting premises.

For further information, contact us on 678-585-9520 or as info@joventech.com.